

**PERANCANGAN DAN IMPLEMENTASI *VIRTUAL  
PRIVATE NETWORK* DENGAN MIKROTIK**

**SKRIPSI**



Oleh  
**Eko Syah Putra Siahaan**  
**140210278**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN KOMPUTER  
UNIVERSITAS PUTERA BATAM  
TAHUN 2021**

**PERANCANGAN DAN IMPLEMENTASI *VIRTUAL  
PRIVATE NETWORK* DENGAN MIKROTIK**

**SKRIPSI**

**Untuk memenuhi salah satu syarat  
memperoleh gelar Sarjana**



**Oleh  
Eko Syah Putra Siahaan  
140210278**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN KOMPUTER  
UNIVERSITAS PUTERA BATAM  
TAHUN 2021**

## **SURAT PERNYATAAN ORISINALITAS**

Yang bertanda tangan dibawah ini saya:

Nama : Eko Syah Putra Siahaan  
NPM : 140210278  
Fakultas : Teknik dan Komputer  
Program Studi : Teknik Informatika

Menyatakan bahwa “Skripsi” yang saya buat dengan judul:

### **PERANCANGAN DAN IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* DENGAN MIKROTIK**

Adalah hasil karya saya sendiri dan bukan “duplikasi” dari karya orang lain. Sepengetahuan saya, di dalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undang yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 23 Juli 2021



**Eko Syah Putra Siahaan**

**NPM:140210278**

**PERANCANGAN DAN IMPLEMENTASI *VIRTUAL  
PRIVATE NETWORK* DENGAN MIKROTIK**

**SKRIPSI**

**Untuk memenuhi salah satu syarat  
memperoleh gelar Sarjana**

**Oleh  
Eko Syah Putra Siahaan  
140210278**

**Telah disetujui oleh Pembimbing pada tanggal  
seperti tertera di bawah ini**

**Batam, 23 Juli 2021**

A handwritten signature in blue ink, appearing to be 'Cosmas Eko Suharyanto', written over a horizontal line.

**Cosmas Eko Suharyanto, S.Kom., M.MSI.  
Pembimbing**

## ABSTRAK

Teknologi jaringan komputer selalu menjadi kebutuhan diberbagai setiap perusahaan yang ada. Cv. Celcomindo merupakan perusahaan yang bergerak dibidang IT yang memanfaatkan teknologi jaringan internet maupun jaringan lokal dalam mengolah data untuk mempermudah pekerjaan dikantor. Permasalahan yang ada dipenelitian ini belum adanya perancangan *virtual private network* diperusahaan Cv. Celcomindo yang akan digunakan untuk pengiriman data atau *remote access* perangkat yang berada dijaringan lokal kantor dapat sepenuhnya diakses dan dikontrol dari luar lingkup lokasi kantor. Dimasa pandemi Covid-19 atau bahkan sudah new normal, pemerintah menghimbau agar menerapkan *Work From Home* dengan bekerja dari rumah masing-masing. Penelitian ini bertujuan untuk merancang sebuah *Virtual Private Network* di perusahaan Cv. Celcomindo yang akan digunakan perusahaan tersebut agar dapat mengolah data, remote akses perangkat, dan mengakses suatu data yang berada pada jaringan lokal kantor tersebut dari lokasi jarak jauh. Metode pengumpulan data pada penelitian ini dilakukan secara Observasi, dengan mengamati atau meninjau secara langsung kelokasi kantor penelitian untuk mengetahui kondisi desain topologi jaringan yang sudah digunakan sebelumnya serta perangkat apa saja yang digunakan oleh perusahaan tersebut. Metode *Virtual Private Network* yang sudah dikonsultasikan dengan direktur pemilik perusahaan menggunakan metode protocol L2TP/IPSec atau *Layer 2 Tunneling Protocol* dan IPSec. Hasil penelitian skripsi ini, dengan memanfaatkan Ip Publik pada perangkat mikrotik dapat dirancangnya *virtual private network* dan perangkat jaringan yang berada dijaringan lokal dapat saling terhubung serta *remote access* berjalan dengan baik. Pengujian yang dilakukan diantaranya dengan mencoba koneksi *virtual private network*, mengakses beberapa perangkat jaringan yang berada dikantor serta pengujian pertukaran atau pengambilan data pada perangkat laptop yang berada dijaringan lokal kantor dapat sepenuhnya diakses oleh *user* yang berada diluar lingkup lokasi kantor. Kesimpulan penelitian yang ditemukan, penerapan VPN sangat mendukung kegiatan aktifitas kantor untuk mengakses data yang berada dijaringan lokal dapat sepenuhnya diakses dari jarak jauh.

**Kata Kunci:** *Virtual Private Network*; MikroTik; *Remote Access*; L2tp/IPSec.

## **ABSTRACT**

*Computer network technology has always been a necessity in every company that exists. Cv. Celcomindo is a company engaged in IT that utilizes internet network technology and local networks in processing data to facilitate office work. The problem in this research is that there is no virtual private network design in the company Cv. Celcomindo which will be used for data transmission or remote access of devices located in the local office network can be fully accessed and controlled from outside the scope of the office location. During the Covid-19 pandemic or even the new normal, the government urges the government to implement Work From Home by working from their respective homes. This study aims to design a Virtual Private Network in the company Cv. Celcomindo, which will be used by the company to process data, remotely access devices, and access data on the local office network from a remote location. The data collection method in this study was carried out by observation, by observing or reviewing directly to the location of the research office to find out the condition of the network topology design that had been used previously and what devices were used by the company. The Virtual Private Network method that has been consulted with the director of the company owner uses the L2TP/IPSec protocol method or Layer 2 tunneling protocol and IPSec. The results of this thesis research, by utilizing the Public Ip on the mikrotik device, it is possible to design a virtual private network and network devices on the local network can be connected to each other and remote access runs well. Tests carried out include trying virtual private network connections, accessing several network devices in the office and testing the exchange or retrieval of data on laptop devices on the local office network that can be fully accessed by users who are outside the scope of the office location. The conclusion of the research found, the application of VPN strongly supports office activities to access data on the local network that can be fully accessed remotely.*

**Keyword:** *Virtual Private Network; Mikrotik; Remote Access; L2tp/IPSec.*

## KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat segera menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan perkuliahan program strata satu (S1) pada Program Studi Teknik Informatika diperguruan tinggi Universitas Putera Batam.

Penulis mengetahui dan sadar bahwa skripsi ini masih jauh dari kata sempurna. Karena itu, kritik dan saran yang diberikan akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis juga menyadari bahwa skripsi ini tidak akan terwujud dan selesai tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Ibu Dr. Nur Elfi Husda, S.Kom., M.SI selaku Rektor Universitas Putera Batam;
2. Bapak Welly Sugianto, S.T., M.M. selaku Dekan Fakultas Teknik Informatika;
3. Bapak Andi Maslan, S.T., M.SI. selaku ketua Program Studi Teknik Informatika;
4. Bapak dosen Cosmas Eko Suharyanto, S.Kom., M.MSI. selaku pembimbing akademik dan pembimbing skripsi pada Program Studi Teknik Informatika Universitas Putera Batam;

5. Seluruh Dosen Teknik Informatika dan Staff Universitas Putera Batam;
6. Bapak Ariston Sitanggang, S.Kom. selaku direktur utama dilokasi penelitian kantor Cv. Celcomindo;
7. Ibu Erita Panjaitan selaku Orang Tua penulis;
8. Irma Sarinah Siahaan selaku Kakak penulis;
9. Tomuan Siahaan selaku Abang penulis.

Semoga Tuhan Yang Maha Esa membalas kebaikan, memberikan kesehatan, keselamatan, rezeki, dan memberkati kita semua, Amin.

Batam, 10 Juli 2021

Eko Syah Putra Siahaan



## DAFTAR ISI

	Halaman
<b>HALAMAN SAMPUL</b> .....	i
<b>HALAMAN JUDUL</b> .....	ii
<b>SURAT PERNYATAAN ORISINALITAS</b> .....	iii
<b>HALAMAN PENGESAHAN</b> .....	iv
<b>ABSTRAK</b> .....	v
<b>ABSTRACT</b> .....	vi
<b>KATA PENGANTAR</b> .....	vii
<b>DAFTAR ISI</b> .....	ix
<b>DAFTAR GAMBAR</b> .....	xiii
<b>DAFTAR TABEL</b> .....	xxi
<b>BAB I PENDAHULUAN</b> .....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah.....	6
1.3 Batasan Masalah.....	6
1.4 Rumusan Masalah .....	7
1.5 Tujuan Penelitian.....	8
1.6 Manfaat Penelitian .....	8
1.6.1 Manfaat Teoritis .....	9
1.6.2 Manfaat Praktis.....	9

<b>BAB II TINJAUAN PUSTAKA .....</b>	<b>10</b>
2.1 Teori Dasar .....	10
2.1.1 Jaringan Komputer .....	10
2.1.2 Standar Jaringan Komputer .....	11
2.1.3 Jenis Jaringan Komputer .....	16
2.1.4 Model OSI Layer .....	20
2.2 Teori Khusus .....	23
2.2.1 Router Mikrotik .....	24
2.2.2 <i>Virtual Private Network</i> .....	26
2.2.3 <i>Tunnel</i> .....	26
2.3 Tools.....	28
2.3.1 Mikrotik RouterBoard RB750 .....	28
2.3.2 Tp Link Wi-Fi Router Archer C24.....	29
2.3.3 WinBox .....	30
2.3.4 Kabel UTP dan RJ45 .....	31
2.4 Penelitian Terdahulu .....	32
2.5 Kerangka Pemikiran.....	35
<b>BAB III METODE PENELITIAN .....</b>	<b>37</b>
3.1 Desain Penelitian.....	37
3.1.1 Identifikasi Masalah .....	38

3.1.2	Rumusan Masalah dan Tujuan.....	38
3.1.3	Studi Literatur.....	38
3.1.4	Observasi.....	38
3.1.5	Analisis Jaringan Lama.....	39
3.1.6	Perancangan Jaringan Sesuai Topologi.....	39
3.1.7	Implementasi Jaringan VPN.....	39
3.1.8	Pengujian.....	40
3.1.9	Hasil Kesimpulan dan Saran.....	41
3.2	Analisis Jaringan Lama atau Yang Sedang Berjalan.....	41
3.2.1	Topologi Jaringan Yang Sedang Berjalan.....	42
3.2.2	Spesifikasi Hardware dan Software Yang Sedang Dipakai.....	43
3.3	Rancangan Jaringan Yang Dibangun atau Diusulkan.....	44
3.3.1	Topologi Jaringan Yang Baru.....	45
3.3.2	Spesifikasi Hardware Dan Software.....	46
3.3.3	Tahapan Rencana Implementasi Jaringan.....	47
3.3.4	Perbedaan Jaringan Yang Lama Dengan Yang Baru.....	48
3.4	Lokasi dan Jadwal Penelitian.....	49
3.4.1	Lokasi.....	50
3.4.2	Jadwal Penelitian.....	51
	<b>BAB IV HASIL DAN PEMBAHASAN.....</b>	<b>52</b>

4.1	Implementasi Hasil Penelitian .....	52
4.1.1	Tahapan Menghubungkan Perangkat .....	52
4.1.2	Tahapan Setting Virtual Private Network .....	121
4.2	Pembahasan .....	127
4.2.1	Pengujian Koneksi Virtual Private Network .....	127
4.2.2	Pengujian Akses Mikrotik Melalui Virtual Private Network .....	135
4.2.3	Pengujian Ping Pada Perangkat Dijaringan Lokal.....	140
4.2.4	Pengujian Akses Tp-Link Melalui Virtual Private Server .....	142
4.2.5	Pengujian Remote Desktop Melalui Virtual Private Network ....	143
	<b>BAB V SIMPULAN DAN SARAN .....</b>	<b>149</b>
5.1	Simpulan .....	149
5.2	Saran.....	150
	<b>DAFTAR PUSTAKA .....</b>	<b>151</b>
	<b>LAMPIRAN .....</b>	<b>154</b>

## DAFTAR GAMBAR

Gambar 2. 1 Jaringan Komputer.....	11
Gambar 2. 2 Organisasi IETF .....	12
Gambar 2. 3 Organisasi ITU.....	12
Gambar 2. 4 Organisasi ISO .....	13
Gambar 2. 5 Organisasi ANSI.....	14
Gambar 2. 6 Organisasi IEEE.....	14
Gambar 2. 7 Organisasi EIA.....	15
Gambar 2. 8 Organisasi FCC .....	15
Gambar 2. 9 Jaringan LAN.....	17
Gambar 2. 10 Jaringan MAN.....	17
Gambar 2. 11 Jaringan WAN .....	18
Gambar 2. 12 Jaringan Server-Client .....	18
Gambar 2. 13 Jaringan Peer to Peer .....	19
Gambar 2. 14 Jaringan Komputer Menggunakan Kabel.....	19
Gambar 2. 15 Jaringan Komputer Menggunakan Wireless .....	20
Gambar 2. 16 Model OSI Layer .....	21
Gambar 2. 17 Simbol Router .....	24
Gambar 2. 18 Mikrotik RB750.....	25
Gambar 2. 19 Mikrotik RB800.....	26
Gambar 2. 20 Perangkat MikroTik RB750.....	29
Gambar 2. 21 Perangkat Tp Link Wi-Fi Router.....	30
Gambar 2. 22 Tampilan WinBox Ketika Login Kemikrotik .....	31

Gambar 2. 23 Kabel UTP Cat 5e dan Rj45.....	32
Gambar 2. 24 Kerangka Pemikiran .....	36
Gambar 3. 1 Desain Penelitian .....	37
Gambar 3. 2 Topologi Jaringan Yang Sedang Digunakan .....	42
Gambar 3. 3 Topologi Jaringan Yang Akan Dirancang.....	45
Gambar 3. 4 Topologi Jaringan Virtual Private Network.....	49
Gambar 3. 5 Kantor CV. Celcomindo.....	50
Gambar 3. 6 Lokasi Penelitian Melalui Google Map.....	50
Gambar 4. 1 Reset ZTE F609 .....	53
Gambar 4. 2 Port Ethernet 1 ZTE Terhubung Dengan Kabel UTP .....	53
Gambar 4. 3 Port Ethernet 1 Mikrotik Terhubung Dengan Kabel UTP .....	54
Gambar 4. 4 Mikrotik Telah Terhubung Ke ZTE F609 dan Laptop .....	55
Gambar 4. 5 Reset MikroTik RB750 .....	56
Gambar 4. 6 Membuka Aplikasi WinBox 65bit Versi 3.27 Dilaptop .....	56
Gambar 4. 7 Tampilan Aplikasi WinBox .....	57
Gambar 4. 8 Mengisi Parameter WinBox Untuk Login .....	58
Gambar 4. 9 Remove Configuration .....	59
Gambar 4. 10 Login Kembali Setelah Konfigurasi MikroTik Dihapus.....	60
Gambar 4. 11 Langkah Kemenu Identity .....	61
Gambar 4. 12 Mengisi Nama Identity.....	61
Gambar 4. 13 Langkah Kemenu Users Login .....	62
Gambar 4. 14 Membuat Akses Login Yang Baru .....	63
Gambar 4. 15 Form User List Untuk Login.....	64

Gambar 4. 16 Menghapus Login Yang Menggunakan Admin .....	64
Gambar 4. 17 Tampilan User List Hanya Celcomindo .....	65
Gambar 4. 18 Langkah Disconnect Agar Login Kembali .....	65
Gambar 4. 19 Login Dengan User Yang Baru .....	66
Gambar 4. 20 Menambahkan Bridge-WAN .....	68
Gambar 4. 21 Tampilan Bridge-WAN Yang Dibuat .....	68
Gambar 4. 22 Menambahkan Bridge Port Untuk Bridge-WAN .....	69
Gambar 4. 23 Tampilan Bridge Port Yang Dibuat Untuk Bridge-WAN.....	70
Gambar 4. 24 Langkah-langkah Kemenu Services .....	71
Gambar 4. 25 Tampilan IP Service List.....	71
Gambar 4. 26 Menutup Beberapa Port Diform IP Service List.....	72
Gambar 4. 27 Tampilan Port Yang Sudah Ditutup atau Disable .....	73
Gambar 4. 28 Langkah Kemenu Addresses.....	73
Gambar 4. 29 Menambahkan IP Publik Statik Di address List .....	74
Gambar 4. 30 Tampilan IP Publik Yang Ditambahkan .....	75
Gambar 4. 31 Langkah-langkah Kemenu Form DNS Setting .....	75
Gambar 4. 32 Tampilan Mengisi Parameter DNS Setting .....	76
Gambar 4. 33 Langkah-langkah Menuju Form Firewall NAT.....	77
Gambar 4. 34 Parameter Pada Menu General Untuk Menambahkan NAT .	78
Gambar 4. 35 Parameter Pada Menu Action Untuk Menambahkan NAT ..	78
Gambar 4. 36 Rule NAT Telah Ditambahkan .....	79
Gambar 4. 37 Langkah Menampilkan Form Route List .....	79
Gambar 4. 38 Tampilan Routes Diform Route List .....	80

Gambar 4. 39 Menambahkan Route Untuk Gateway WAN atau Internet ..	81
Gambar 4. 40 Tampilan Penambahan Routes Pada WAN .....	81
Gambar 4. 41 Langkah Membuka Form Terminal.....	82
Gambar 4. 42 Tampilan Form Terminal .....	82
Gambar 4. 43 Pengujian Ping MikroTik Keinternet .....	83
Gambar 4. 44 Langkah Kemenu Bridge .....	84
Gambar 4. 45 Tampilan Form Bridge .....	84
Gambar 4. 46 Langkah Menambahkan Bridge-LAN .....	85
Gambar 4. 47 Tampilan Bridge-WAN dan Bridge-LAN Diform Bridge....	86
Gambar 4. 48 Langkah Menambahkan Bridge Port Untuk Bridge-LAN ....	87
Gambar 4. 49 Tampilan Bridge Port Di Bridge-WAN dan Bridge-LAN ....	88
Gambar 4. 50 Langkah-langkah Menampilkan Form Address List .....	89
Gambar 4. 51 Tampilan Form Address List .....	89
Gambar 4. 52 Menambahkan IP Address Untuk Jaringan Lokal .....	90
Gambar 4. 53 Tampilan Form Address List .....	91
Gambar 4. 54 Langkah-langkah Membuka Form DHCP Server .....	92
Gambar 4. 55 Tampilan Form DHCP Server .....	92
Gambar 4. 56 Langkah-langkah DHCP Setup.....	93
Gambar 4. 57 Mengisi DHCP Address Space .....	94
Gambar 4. 58 Mengisi Gateway DHCP Network .....	94
Gambar 4. 59 Mengisi Parameter Addresses to Give Out .....	95
Gambar 4. 60 Mengisi DNS Server pada DHCP Setup .....	95
Gambar 4. 61 Mengisi Parameter Lease Time DHCP Setup.....	96



Gambar 4. 62 DHCP Server Berhasil Dibuat .....	96
Gambar 4. 63 Langkah-langkah Menuju Form IP Pool.....	97
Gambar 4. 64 Tampilan Form IP Pool .....	98
Gambar 4. 65 Langkah-langkah Menampilkan Form Route List.....	98
Gambar 4. 66 Tampilan Form Route List .....	99
Gambar 4. 67 Langkah-langkah Membuka Aplikasi CMD Dilaptop .....	100
Gambar 4. 68 Tampilan CMD Dengan Ketik Perintah Ipconfig.....	100
Gambar 4. 69 Tampilan CMD Dengan Ketik Perintah Ipconfig /all .....	101
Gambar 4. 70 Tampilan Pengujian Ping Google Dari Perangkat Laptop ..	102
Gambar 4. 71 Laptop Dapat Terhubung Kejaringan Internet .....	102
Gambar 4. 72 Menambahkan Port Ether 3 Pada Bridge-LAN .....	104
Gambar 4. 73 Tampilan Bridge Port Yang Sudah Dibuat .....	104
Gambar 4. 74 Bridge Port 1 Sampai 5 MikroTik Sudah Dibuat .....	106
Gambar 4. 75 Perangkat Tp Link Wi-Fi Router Sebagai Access Point .....	106
Gambar 4. 76 Ethernet Yang Terdapat Pada Tp link .....	107
Gambar 4. 77 Menghubungkan Tp Link dan Laptop Menggunakan UTP	107
Gambar 4. 78 Reset Perangkat Tp Link .....	108
Gambar 4. 79 Kondisi Lampu Led Tp Link Ketika Direset .....	108
Gambar 4. 80 Memeriksa IP Address Pada Laptop dan Tp Link.....	109
Gambar 4. 81 Mengakses Tp Link Dengan IP 192.168.0.1.....	110
Gambar 4. 82 Memasukkan Password Baru Untuk Login Ke Tp Link .....	110
Gambar 4. 83 Tampilan Menu Tp Link .....	111
Gambar 4. 84 Setting Tp Link Menjadi Access Point .....	111

Gambar 4. 85 Tampilan Reboot Tp Link .....	112
Gambar 4. 86 Halaman Login Tp Link Setelah Reboot .....	112
Gambar 4. 87 Mengisi Parameter Wireless Setting .....	113
Gambar 4. 88 Halaman Confirm Setting Pada Wireless Setting .....	113
Gambar 4. 89 Menyelesaikan Quick Setup Pada Tp Link .....	114
Gambar 4. 90 Tampilan Menu Internet Ketika Tp Link Mode Router .....	115
Gambar 4. 91 Tampilan Menu Internet Saat Tp Link Mode Access Point .....	115
Gambar 4. 92 Setting LAN Tp-Link Secara Dynamic IP .....	116
Gambar 4. 93 DHCP Server Pada Tp Link Disable .....	116
Gambar 4. 94 Setting Wireless 2.4 GHz Pada Tp Link .....	117
Gambar 4. 95 Setting Wireless 5 GHz Pada Tp Link .....	117
Gambar 4. 96 Tp Link Terhubung Ke MikroTik Dengan Kabel UTP .....	118
Gambar 4. 97 Memeriksa Bridge Port Ether 3 Pada MikroTik .....	119
Gambar 4. 98 Langkah-langkah Menampilkan Form DHCP Server .....	119
Gambar 4. 99 Tampilan Menu Leases Di form DHCP Server .....	120
Gambar 4. 100 Login MikroTik Menggunakan WinBox .....	121
Gambar 4. 101 Langkah-langkah Menampilkan Form IP Pool .....	122
Gambar 4. 102 Langkah-langkah Menambahkan IP Pool VPN .....	123
Gambar 4. 103 Mengisi Parameter Profile VPN Di menu General .....	124
Gambar 4. 104 Mengisi Parameter Di menu Protocols .....	124
Gambar 4. 105 Mengisi Parameter Di menu Limits .....	125
Gambar 4. 106 Tampilan Profile VPN Telah Ditambahkan .....	125
Gambar 4. 107 Membuat Secret Di form PPP .....	126

Gambar 4. 108 Mengaktifkan dan Mengisi Parameter Pada L2TP Server	127
Gambar 4. 109 Menghubungkan Laptop Dengan Wi-Fi Smartphone .....	128
Gambar 4. 110 Memeriksa IP Address Yang Didapat Laptop .....	129
Gambar 4. 111 Melakukan Ping Google Pada CMD .....	129
Gambar 4. 112 Pengujian Laptop Mengakses Internet .....	130
Gambar 4. 113 Langkah-langkah Menuju Ke VPN Setting .....	131
Gambar 4. 114 Menambahkan Jaringan VPN .....	131
Gambar 4. 115 Mengisi Parameter VPN yang akan ditambahkan .....	132
Gambar 4. 116 Menghubungkan Laptop Ke VPN Kantor .....	133
Gambar 4. 117 Mengisi Parameter Sign In Ketika Connecting .....	133
Gambar 4. 118 Laptop Terhubung Dengan VPN Kantor .....	134
Gambar 4. 119 Memeriksa IP Address Laptop Dengan CMD .....	135
Gambar 4. 120 Remote MikroTik Melalui VPN Dengan IP 172.16.1.1 ...	136
Gambar 4. 121 Remote MikroTik Berhasil Menggunakan IP 172.16.1.1 .	137
Gambar 4. 122 Tampilan L2TP Server Sedang Aktif Pada Form PPP .....	137
Gambar 4. 123 Menu Active Connections Menunjukkan VPN Aktif .....	138
Gambar 4. 124 VPN Server dan Client Sedang Aktif Diroutes .....	138
Gambar 4. 125 Remote MikroTik Melalui VPN Dengan IP 192.168.1.1 .	139
Gambar 4. 126 MikroTik Dapat Diremote Dengan IP 192.168.1.1 .....	139
Gambar 4. 127 Perangkat Yang Sedang Terhubung Kejaringan Lokal .....	140
Gambar 4. 128 Ping 192.168.1.97 Keperangkat Cctv Camera .....	141
Gambar 4. 129 Ping 192.168.1.98 Keperangkat Tp Link .....	141
Gambar 4. 130 Ping 192.168.1.101 Keperangkat Printer .....	142

Gambar 4. 131 Mengakses Port 80 Http Pada Tp Link Berhasil diremote	143
Gambar 4. 132 Memeriksa IP Address Perangkat Yang Akan Diremote..	144
Gambar 4. 133 Langkah Membuka Aplikasi Remote Desktop .....	144
Gambar 4. 134 Mengisi Parameter Pada Remote Desktop.....	145
Gambar 4. 135 Mengisi Parameter Password Untuk Remote Laptop.....	146
Gambar 4. 136 Tampilan Pop Up Akan Muncul.....	146
Gambar 4. 137 Proses Connecting Kelaptop Yang Diremote .....	147
Gambar 4. 138 Tampilan Desktop Laptop Yang Diremote .....	147
Gambar 4. 139 Tampilan Pengujian RDP Untuk Pertukaran File.....	148

## **DAFTAR TABEL**

Tabel 2. 1 Spesifikasi MikroTik Yang Digunakan.....	28
Tabel 2. 2 Spesifikasi Tp Link Wi-Fi Router Yang Digunakan.....	30
Tabel 3. 1 Spesifikasi Hardware dan Software Yang Digunakan .....	44
Tabel 3. 2 Spesifikasi Hardware dan Software Yang Digunakan .....	47
Tabel 3. 3 Jadwal Penelitian .....	51

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi jaringan komputer sangatlah pesat dan selalu menjadi kebutuhan sebagian besar perusahaan perkantoran yang berguna untuk mempermudah pengolahan dan pengiriman suatu data antar beberapa komputer dan perangkat lain nya. Dengan memanfaatkan teknologi jaringan komputer pihak pengguna memperoleh berbagai fungsi serta keuntungan dalam hal berkomunikasi, pertukaran data menjadi lebih mudah, mengurangi resiko rusaknya data, menghemat waktu, serta mempermudah suatu pekerjaan yang dilakukan.

Mengenai jaringan komputer, terdapat suatu sistem pendukung untuk mendukung suatu jaringan dalam hal berkomunikasi, bertukar informasi dan sebagai nya yaitu *virtual private network* atau disingkat VPN. Penggunaan VPN ini salah satu cara dimana pengiriman atau penerimaan suatu paket antara beberapa jaringan yang terhubung dilakukan secara terenkripsi atau bersifat rahasia dengan memanfaatkan jalur jaringan internet. Penggunaan VPN ini berkaitan dengan proses *tunneling* yang akan digunakan untuk membuat suatu aliran paket dilakukan secara aman pada jaringan yang sering disebut *Tunneling Protocol*. Misal nya terdapat jaringan komputer lokal di perusahaan A yang akan dihubungkan dengan jaringan komputer yang berada dilokasi B dengan jarak yang cukup jauh. Jarak antara lokasi A dan B tersebut sangat jauh dan untuk

menghubungkan ke dua lokasi tersebut dibutuhkan pengkabelan jaringan yang sangat panjang dan sangat jauh lokasi nya. Untuk mengatasi hal tersebut, perancangan *virtual private network* sebagai solusi nya melalui perantara jaringan *internet* dimana tidak memerlukan kabel yang sangat panjang untuk menghubungkan jaringan komputer diantara 2 lokasi perusahaan tersebut.

Peristiwa yang kita ketahui saat ini, terdapat wabah virus corona yang membuat hampir diseluruh bagian negara didunia ini melakukan penerapan *lockdown* atau *Work From Home* yang bertujuan untuk menanggulangi penyebaran virus corona. Salah satunya negara Indonesia menerapkan bekerja secara *Work From Home*. Karyawan pekerja harus menyelesaikan pekerjaan kantornya dari rumah masing-masing dengan tujuan menanggulangi penyebaran wabah virus corona yang sedang terjadi. Dari fenomena ini, untuk mengakses segala jenis data pada jaringan komputer lokal yang ada dikantor perlu dirancangnya *virtual private network* atau disingkat VPN agar pengguna bisa lebih mudah mengakses atau mengolah data diluar lingkup area kantor tersebut. Sebelum ada nya wabah ini, penerapan VPN dalam suatu jaringan juga sudah banyak diterapkan diperusahaan-perusahaan besar antara pusat dan cabang. Pada beberapa kampus juga diterapkan, antara lokasi suatu pusat kampus dengan cabang kampus yang menerapkan VPN dengan tujuan agar komputer jaringan dapat saling terhubung.

Misalnya pada perusahaan terdapat suatu permasalahan mengenai jaringan komputer lokal atau permasalahan suatu aplikasi disalah satu komputer karyawan yang berada dikantor tersebut, sedangkan staff teknisi yang ahli menangani situasi

itu sudah pulang kerja atau sedang berada di posisi luar area kantor. Keadaan mendesak seperti ini, staff tersebut diharuskan memantau permasalahan yang sedang terjadi. Kondisi seperti ini sangat membutuhkan sistem *virtual private network* supaya staff teknisi dapat melakukan *remote access* atau memantau dari jarak jauh terhadap perangkat yang berada di jaringan lokal atau komputer yang sedang bermasalah tersebut agar dapat ditangani. Contoh kasus permasalahan lainnya juga banyak ditemukan diberbagai perusahaan, seperti hal nya antara lokasi pusat perusahaan dengan lokasi cabang perusahaan yang letak nya berjauhan. Situasi seperti ini memungkinkan untuk merancang sebuah *virtual private network* agar dalam hal pertukaran data antara jaringan lokal di lokasi kantor pusat dan di lokasi kantor cabang bisa dilakukan sebaik dan semudah mungkin. Sistem jaringan komputer yang aman dan dapat mengatasi permasalahan seperti ini, solusinya dengan merancang *virtual private network* yang dapat membuat jaringan komputer lokal yang lokasinya berjauhan dapat saling terkoneksi seakan-akan kedua jaringan tersebut di dalam suatu jaringan internet yang besar. Teknologi *virtual private network* ini memungkinkan setiap pengguna atau *user* untuk dapat mengakses jaringan lokal dari jangkauan diluar area kantor dengan melibatkan jalur internet sebagai perantaranya. Melalui *virtual private network*, maka pengguna atau *user* dapat mengakses sumber daya atau *resource* yang berada di jaringan lokal kantor untuk mendapatkan hak akses walau posisi user sedang tidak berada di kantor. Tidak lepas dari keamanan data dan kerahasiaan data yang melintas melalui internet, VPN selalu disertakan akan fitur utama yaitu enkripsi pada penggunaan *tunneling protocol* yang digunakan.



Fenomena yang diuraikan diatas, peneliti menemukan suatu permasalahan yang ada pada CV. Celcomindo. Perusahaan ini merupakan salah satu perusahaan yang bergerak dalam bidang IT Konsultan. Perusahaan tersebut menerapkan anjuran pemerintah untuk mencegah penularan wabah virus corona dengan menjadwalkan karyawannya bekerja bergiliran dari rumah masing-masing atau disebut *Work From Home*. Untuk pekerjaan kantor yang dilakukan dilokasi rumah masing-masing, tentu terdapat suatu permasalahan seperti halnya karyawan kesulitan mengakses, mengolah, ataupun memproses data yang ada di jaringan lokal kantor tersebut. Kemudian terdapat juga permasalahan dikantor CV. Celcomindo tersebut ketika staff teknisi sedang tidak berada dikantor atau bahkan direktur pemilik perusahaan sedang berada diluar kota, yang bersangkutan tidak dapat melakukan *remote access* atau memantau dari jarak jauh terhadap situasi permasalahan yang sedang terjadi di jaringan lokal kantor tersebut. Dari permasalahan yang ditemukan peneliti di kantor CV. Celcomindo, perlu nya di rancang *virtual private network* untuk mengatasi hal-hal seperti yang disebutkan diatas. Penulis akan mengangkat permasalahan ini, bahwa perusahaan tersebut belum membangun dan merancang *virtual private network* yang bertujuan agar pengguna dapat saling terhubung dan mengelola suatu data atau perangkat yang ada di jaringan lokal perusahaan dengan *remote access* dari jarak jauh.

Peneliti perlu memperhatikan secara umum mengenai kondisi jaringan komputer sebelumnya yang sudah ada di CV. Celcomindo tersebut. Jaringan komputer yang dianalisa dikantor tersebut, struktur jaringan komputer yang ada terdapat sebuah modem ISP ZTE F609 yang digunakan agar jaringan lokal kantor

dapat terhubung ke jaringan internet. Perangkat-perangkat yang berada di kantor terhubung ke modem zte f609 melalui media perantara *wireless* atau *wi-fi*. Perangkat-perangkat yang terhubung di jaringan lokal diantaranya terdapat 1 komputer direktur yang digunakan untuk menyimpan segala *file* laporan pekerjaan kantor, 2 buah perangkat laptop yang digunakan karyawan, dan 1 buah perangkat printer. Setelah menganalisis jaringan lama yang ada di kantor, peneliti akan mengusulkan bentuk topologi jaringan yang akan dirancang dalam perancangan *virtual private network* ini. Perangkat yang dibutuhkan untuk merancang *virtual private network* dengan menambahkan *router* MikroTik RB750 dan Tp Link Wi-Fi Router yang akan dijadikan sebagai akses poin karena MikroTik RB750 tidak memiliki fasilitas *wi-fi*. Direktur lokasi penelitian menginginkan agar perangkat-perangkat yang berada di kantor tetap saling terhubung dengan menggunakan media penghantar *wi-fi*, maka peneliti menggunakan Tp link tersebut sebagai akses poin agar perangkat-perangkat yang berada di kantor tetap dapat saling terhubung menggunakan *wi-fi*. Tantangan yang harus dialami peneliti dalam perancangan ini diantaranya karena penambahan perangkat MikroTik peneliti harus mengonfigurasi jaringan dari awal. Mengonfigurasi MikroTik dengan *ip publik* agar perangkat-perangkat dapat terhubung ke jaringan *internet*, mengonfigurasi alamat *ip address* untuk jaringan lokal, mengonfigurasi Tp-link Wi-Fi Router menjadi akses poin agar perangkat yang berada di kantor dapat saling terhubung menggunakan *wi-fi*, dan merancang *virtual private network* menggunakan MikroTik dengan menggunakan protokol L2tp/IPSec sesuai dengan topologi jaringan yang diusulkan di kantor tersebut.

Permasalahan yang ditemukan peneliti serta tantangan yang akan dialami, peneliti memiliki ketertarikan untuk melakukan penelitian ini yang berlokasi di CV. Celcomindo. Dalam membangun dan merancang *virtual private network* dengan permasalahan yang disampaikan, maka penulis mengangkat judul skripsi **Perancangan dan Implementasi *Virtual Private Network* Dengan Mikrotik**. Metode yang digunakan pada penelitian ini menggunakan protokol L2TP/IPSec atau disebut *Layer 2 Tunneling Protocol/IPSec*.

## **1.2 Identifikasi Masalah**

Berdasarkan kutipan dari latar belakang, identifikasi masalah diuraikan sebagai berikut:

1. Belum dirancangnya *virtual private network* agar dapat melakukan *remote access* pada perangkat jaringan lokal yang berada dikantor.
2. Mengonfigurasi ulang mikrotik untuk jaringan *internet* dan mengonfigurasi Tp Link sebagai akses poin untuk perangkat jaringan lokal yang berada dikantor sesuai dengan topologi jaringan yang diusulkan.
3. Beberapa pengguna atau user masih belum mengetahui dan memahami cara menghubungkan VPN dan melakukan *remote access* keperangkat yang berada di jaringan kantor.

## **1.3 Batasan Masalah**

Untuk menghindari kesulitan yang akan terjadi dalam proses penelitian, maka penelitian ini melakukan batasan masalah sebagai berikut:

1. Perangkat yang digunakan MikroTik RB750 dan Tp Link Wi-Fi Router.
2. Lokasi penelitian dalam perancangan VPN dilakukan di kantor CV. Celcomindo.
3. Konfigurasi MikroTik menggunakan aplikasi WinBox pada perangkat laptop.
4. *Virtual Private Network* yang dirancang menggunakan protokol *Layer 2 Tunneling Protocol* dan IPSec (L2TP/IPSec).
5. Menggambar topologi jaringan menggunakan aplikasi Draw.io.
6. Untuk Ip Publik menggunakan jasa layanan ISP Indihome Astinet.
7. Penelitian yang dilakukan hanya perancangan *virtual private network* dengan tambahan mengonfigurasi MikroTik untuk terhubung ke jaringan *internet* dan konfigurasi Tp Link Wi-Fi Router menjadi akses poin untuk perangkat yang terhubung di jaringan lokal.
8. Pengujian yang dilakukan menguji koneksi *virtual private network*, *remote* MikroTik, melakukan ping pada perangkat yang terhubung di jaringan lokal, *remote* Tp Link Wi-Fi Router, serta pengujian *remote desktop* untuk pertukaran file.

#### **1.4 Rumusan Masalah**

Dari permasalahan yang terdapat pada latar belakang, maka pada bagian rumusan masalah diantaranya sebagai berikut:

1. Bagaimana cara merancang *virtual private network* untuk dapat melakukan *remote access* pada perangkat yang berada di jaringan lokal kantor?

2. Bagaimana cara mengonfigurasi MikroTik dengan menggunakan ip publik untuk terhubung ke jaringan internet dan mengonfigurasi Tp Link sebagai akses poin sesuai dengan topologi jaringan yang diusulkan?
3. Bagaimana agar *user* atau pengguna dapat mengetahui dan memahami cara menghubungkan VPN dan melakukan *remote* perangkat yang berada di jaringan kantor?

### **1.5 Tujuan Penelitian**

Tujuan penelitian yang dilakukan adalah sebagai berikut:

1. Untuk mengetahui cara perancangan *virtual private network* agar dapat melakukan *remote access* pada perangkat yang berada di jaringan kantor.
2. Untuk mengetahui cara menyetting ip publik di MikroTik agar terhubung ke jaringan *internet* dan mengonfigurasi Tp Link sebagai akses poin sesuai topologi jaringan yang diusulkan.
3. Untuk mempermudah pengguna atau user dalam menggunakan VPN yang dirancang dan dapat melakukan *remote access* perangkat yang berada di jaringan kantor.

### **1.6 Manfaat Penelitian**

Manfaat pada penelitian ini terbagi menjadi 2, yaitu manfaat teoritis dan manfaat praktis.

### **1.6.1 Manfaat Teoritis**

1. Sebagai ilmu pengetahuan tambahan bagi seorang *network engineer* atau yang membutuhkan dalam mengembangkan penerapan *virtual private network*.
2. Dapat dijadikan bahan referensi oleh perguruan tinggi universitas.
3. Perusahaan dapat mempelajari atau merancang sendiri jaringan *virtual private network*.

### **1.6.2 Manfaat Praktis**

1. Memudahkan pekerjaan karyawan atau pengguna yang bekerja di CV. Celcomindo dalam mengakses data atau *remote access* walau sedang tidak berada di area kantor.
2. Fasilitas sistem *virtual private network* yang dirancang mendukung perusahaan untuk meningkatkan kinerjanya.
3. Penulis memiliki semangat dan mendapatkan ilmu tambahan atau pengalaman dalam mengembangkan penelitian ini.

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **2.1 Teori Dasar**

Penulis menjabarkan beberapa teori jaringan komputer yang berhubungan dengan pembahasan pada penelitian ini menggunakan referensi resmi yang telah dipublikasikan. Penyusunan karya ilmiah atau dalam melakukan penelitian, harus mengandalkan teori-teori yang ada untuk mendukung suatu penelitian yang sedang dilakukan.

##### **2.1.1 Jaringan Komputer**

Jaringan komputer merupakan sekumpulan komputer yang saling terhubung antara satu dengan yang lainnya menggunakan suatu protokol komunikasi. Melalui media komunikasi tersebut akan memudahkan pengguna dalam menyelesaikan pekerjaannya sehingga dapat saling berbagi atau bertukar informasi.

Pada jaringan komputer, tiap komputer atau perangkat yang saling terhubung dapat saling bertukar data melalui proses data link yang sering disebut media kabel atau nirkabel. Jaringan yang sangat luas dan populer yang diketahui adalah *Internet* (Sofana Iwan, 2017).

Jaringan komputer merupakan sistem yang terdapat komputer-komputer untuk dapat berbagi sumber daya antara satu dengan yang lain, berkomunikasi,

dan dapat mengakses informasi kesuatu server atau antar jaringan itu sendiri (Hidayatulloh & Rahmawati, 2018).

Pembahasan mengenai ilmu jaringan komputer sangat banyak, namun penulis akan menjelaskan secara umumnya saja. Untuk mendalami pemahaman jaringan komputer perlu diketahuinya apa itu jaringan komputer, standar jaringan komputer, jenis jaringan komputer, komponen jaringan, protokol jaringan, pengalamatan IP pada jaringan, mengenal jaringan media kabel bahkan jaringan *wireless*, pengenalan routing, keamanan jaringan, port jaringan dan masih banyak lagi ilmu pengetahuan dalam materi teknologi jaringan ini.



**Gambar 2. 1** Jaringan Komputer

### **2.1.2 Standar Jaringan Komputer**

Jaringan komputer dibangun dengan memperhatikan arsitektur standar yang dibuat oleh lembaga standar industri dunia. Beberapa organisasi badan standarisasi yang ada didunia bertugas untuk mengatur tentang standar komunikasi dalam jaringan komputer sehingga proses komunikasi dapat dilakukan.



### 2.1.2.1 *Internet Engineering Task Force (IETF)*

Organisasi ini salah satu kunci dibalik perkembangan *internet*, organisasi ini tumbuh dan berkembang bersama *internet* dan protokol IP. Organisasi ini tertarik dalam mengembangkan jaringan komputer dan internet yang bertanggung jawab dalam mengatur dan menetapkan protokol standar yang digunakan di jaringan internet.



**Gambar 2. 2** Organisasi IETF

### 2.1.2.2 *International Telecommunications Union (ITU)*

ITU merupakan suatu organisasi yang mempromosikan penggunaan secara global spektrum radio bersama, mendukung kerja sama internasional dalam menjalankan orbit satelit, membantu dalam pengembangan dan koordinasi standar teknis diseluruh dunia, dan bekerja untuk meningkatkan infrastruktur telekomunikasi dinegara berkembang. ITU memiliki tiga sektor, yaitu Standarisasi (ITU-T), komunikasi radio (ITU-R), dan pengembangan (ITU-D).



**Gambar 2. 3** Organisasi ITU

### **2.1.2.3 International Standards Organization (ISO)**

Organisasi ini didirikan pada tahun 1947 sebagai badan yang menerapkan standar-standar internasional yang terdiri dari wakil-wakil dari badan standarisasi nasional di setiap negara. Organisasi ini menetapkan model referensi standar yang disebut OSI atau *Open System Interconnection* yang menerapkan himpunan protokol yang memungkinkan terhubungnya 2 sistem jaringan yang berbeda. OSI ini digunakan untuk menjelaskan proses cara kerja jaringan komputer secara logika.



**Gambar 2. 4** Organisasi ISO

### **2.1.2.4 American National Standards Institute (ANSI)**

Organisasi ini merupakan sebuah lembaga nirlaba swasta yang mengawasi pengembangan standar konsensus sukarela untuk produk, jasa, proses, sistem, dan personel di Amerika Serikat. Lembaga tersebut mengawasi pembuatan, diberlakukannya, dan penggunaan ribuan norma dan pedoman yang secara langsung berdampak bisnis hampir di setiap sektor. Lembaga tersebut juga mengkoordinasikan standar Amerika Serikat dengan standar internasional sehingga produk-produk Amerika Serikat dapat digunakan di seluruh dunia. ANSI ikut serta dalam mendefinisikan standar protokol dalam jaringan, membantu dalam hal komunikasi jaringan, dan memiliki hubungan dengan badan-badan

penentu standar internasional lainnya. ANSI merupakan salah satu anggota IEC dan ISO.



**Gambar 2. 5** Organisasi ANSI

### **2.1.2.5 Institute of Electrical and Electronics Engineers (IEEE)**

IEEE adalah sebuah organisasi profesi yang memiliki banyak ahli di bidang teknik. Fungsi organisasi ini antara lain untuk pengembangan standar-standar komunikasi dan bertindak sebagai pihak yang mempercepat teknologi-teknologi baru dalam aspek industri maupun rekayasa yang mencakup telekomunikasi, jaringan komputer, kelistrikan, antariksa, serta elektronika.



**Gambar 2. 6** Organisasi IEEE

### **2.1.2.6 Telecommunication Industry Association (TIA)**

Suatu organisasi terpisah yang diakui oleh ANSI dan bekerjasama dengan Asosiasi Industri Elektronika (EIA). TIA organisasi terbaik untuk mengembangkan standard pemasangan kabel menggunakan disain dan instalasi sistem pemasangan kabel yang terkoordinasi.



**Gambar 2. 7** Organisasi EIA

### **2.12.7 Federal Communications Commission (FCC)**

Organisasi ini bergerak di bidang telekomunikasi, organisasi independent dan didirikan oleh pemerintah US. Organisasi ini bertujuan untuk mengatur komunikasi wireless agar tidak terjadi kesimpang siuran dan penyalahgunaan sinyal atau frekuensi radio yang digunakan dalam teknologi wireless. Selain itu mengatur dalam penggunaan *frequency*, *bandwidth*, *maximum power of the intentional radiator*, dan *maximum equivalent isotropically radiated power* (EIRP).



**Gambar 2. 8** Organisasi FCC

Ketujuh standar organisasi yang disampaikan mempunyai fungsi dan tujuan masing-masing. Standar jaringan yang saat ini diakui yaitu *The Open System Connection* atau OSI yang dibuat oleh lembaga ISO (*The International Standard*

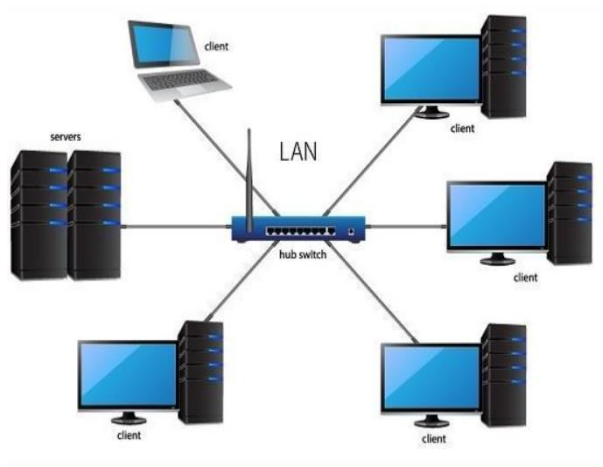
*Organization*), Amerika Serikat. Selain ISO, standarisasi masalah jaringan juga diselenggarakan oleh badan dunia lainnya seperti ITU (*International Telecommunication Union*), ANSI (*American National Standard Institute*), NCITS (*National Committee for Information Technology Standardization*), dan juga lembaga asosiasi profesi IEEE (*Institute of Electrical and Electronics Engineers*) dan ATM-Forum di Amerika (Maslan, 2012). Komputer-komputer yang terhubung dalam jaringan komputer harus memakai aturan komunikasi (*Protocol*) yang sama agar masing-masing komputer dapat berkomunikasi yang baik dengan komputer lainnya.

### **2.1.3 Jenis Jaringan Komputer**

Jaringan komputer dapat dibedakan berdasarkan beberapa kriteria, seperti luas area, media transmisi, pola operasi, dan sebagainya.

#### **2.1.3.1 Berdasarkan luas area atau jangkauan geografis**

A. LAN (*Local Area Network*) jaringan yang terdapat didalam gedung atau kampus yang berjarak sampai dengan beberapa kilometer. LAN sering digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor atau perusahaan untuk dan saling bertukar informasi.



**Gambar 2. 9** Jaringan LAN

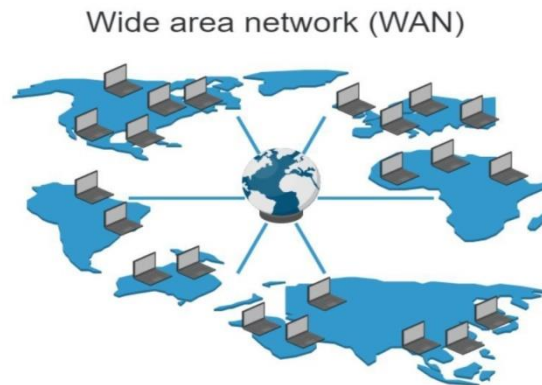
B. MAN (*Metropolitan Area Network*) jaringan versi LAN yang berukuran lebih besar, menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau antar sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi atau umum. MAN juga menunjang data dan suara bahkan dapat digunakan untuk aplikasi TV kabel.

Metropolitan area network (MAN)



**Gambar 2. 10** Jaringan MAN

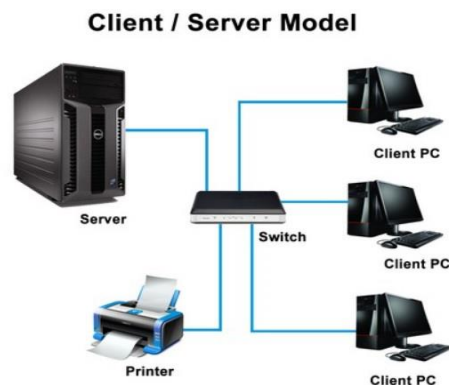
C. WAN (*Wide Area Network*) jangkauan jaringannya mencakup daerah geografis yang luas seringkali mencakup negara bahkan benua. Teknologi yang digunakan hampir sama dengan LAN.



**Gambar 2. 11** Jaringan WAN

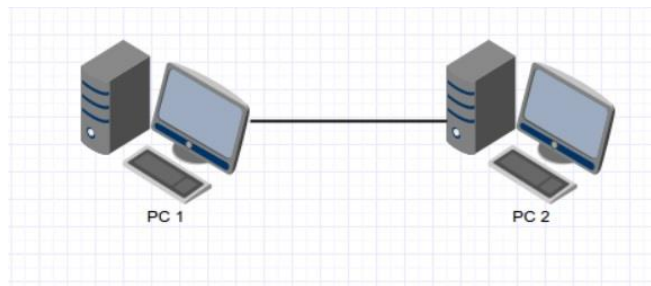
### 2.1.3.2 Berdasarkan pola pengoperasian atau fungsi masing-masing komputer

A. Jaringan *Client-Server* terdapat 1 atau beberapa komputer server dan komputer client. Komputer yang akan menjadi komputer server maupun menjadi komputer client dan diubah-ubah melalui software jaringan pada protokolnya. Komputer client sebagai perantara untuk dapat mengakses data pada komputer server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer client.



**Gambar 2. 12** Jaringan Server-Client

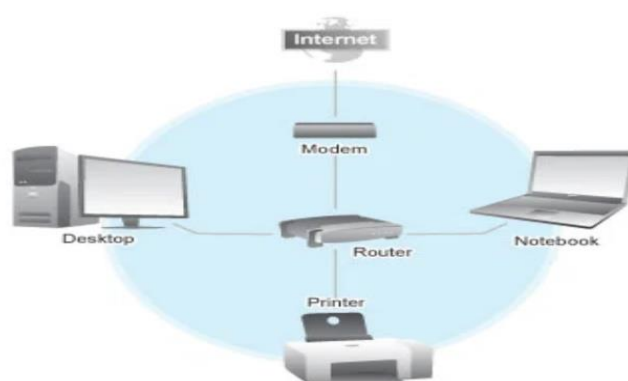
B. Jaringan *Peer to Peer* tidak ada komputer client maupun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi sehingga semua komputer berfungsi sebagai client sekaligus sebagai server.



**Gambar 2. 13 Jaringan Peer to Peer**

### 2.13.3 Berdasarkan media penghantar yang digunakan

A. Jaringan berkabel (*Wire Network* atau *Wireline Network*) untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar komputer jaringan.



**Gambar 2. 14 Jaringan Komputer Menggunakan Kabel**

B. Jaringan nirkabel (*Wireless Network*) Merupakan jaringan dengan menggunakan media penghantar berupa gelombang elektromagnetik atau



radio. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan.

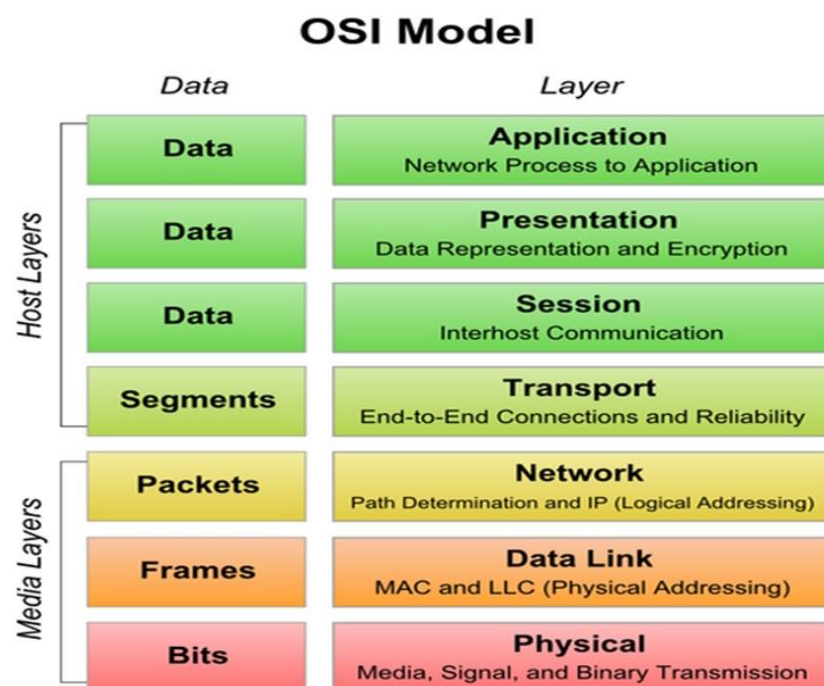


**Gambar 2. 15** Jaringan Komputer Menggunakan Wireless

#### 2.1.4 Model OSI Layer

Pada awal pengembangan jaringan komputer, perusahaan – perusahaan pembuat perangkat jaringan komputer membuat standar mereka sendiri. Sehingga antar perangkat jaringan komputer yang berbeda merk tidak dapat saling berkomunikasi. Untuk mengatasi hal ini maka beberapa organisasi di bidang komputer bekerjasama untuk membuat sebuah standar untuk komunikasi data jaringan komputer. Hasil dari kerjasama ini kemudian dikenal dengan Open System Interconnection (OSI) yang terdiri dari 7 lapisan / layer. Setelah dihasilkannya OSI, maka setiap perusahaan pembuat perangkat jaringan komputer harus mendesain perangkatnya sesuai dengan OSI sehingga meskipun berbeda merk, perangkat jaringan komputer yang terstandar akan dapat saling berkomunikasi.

*Open System Interconnection* atau sering disebut dengan OSI adalah suatu standar komunikasi yang telah ditetapkan antara mesin yang terdiri dari tujuh lapisan. Masing-masing lapisan mempunyai peran dan fungsi yang berbeda-beda satu dengan yang lainnya. Masing-masing layer memiliki tanggung jawab secara khusus pada proses komunikasi data (Maslan, 2012).



**Gambar 2. 16** Model OSI Layer

#### 2.1.4.1 Physical Layer

Pada layer terendah dari OSI Layer, *Physical layer* menerima data dari Data Link layer dan mengubahnya menjadi sinyal pada media transmisi. Tergantung dari media transmisi yang digunakan, apabila menggunakan media transmisi kabel UTP maka *frame* / PDU akan diubah menjadi arus listrik DC. Apabila menggunakan media transmisi *Fiber Optic* maka *frame* / PDU akan diubah

menjadi cahaya. Sedangkan apabila menggunakan media transmisi nirkabel maka *frame* / PDU akan diubah menjadi gelombang radio (Prakasa, 2018).

#### **2.14.2 Data Link Layer**

*Data Link Layer* merupakan lapisan yang akan memberikan informasi *Media Access Control (MAC) Address* pada paket data yang melalui lapisan ini. *MAC Address* merupakan identitas dari *Network Card* yang terdiri dari 48-bit angka heksadesimal. 6 bit pertama dari *MAC Address* merupakan informasi dari pembuat *Network Card* dan sisanya merupakan kode unik dari *Network Card* tersebut. Informasi *MAC Address* akan disimpan di perangkat yang terhubung ke jaringan komputer seperti komputer, *router*, *switch* dll yang disebut dengan tabel *Address Resolution Protocol* (Prakasa, 2018).

#### **2.14.3 Network Layer**

Lapisan ini mengatur tentang alamat *Internet Protocol (IP Address)* dari sebuah perangkat yang terhubung ke jaringan komputer. *IP Address* merupakan identitas dari perangkat yang terhubung ke jaringan komputer sehingga pertukaran data dapat dilakukan. Secara umum *IP Address* dibagi menjadi 2 kelompok yaitu *IP Address Public* dan *Local*. *IP Address Public* adalah alamat sebuah perangkat jaringan komputer (server / router) yang dapat diakses secara langsung melalui koneksi internet (Prakasa, 2018).

#### **2.14.4 Transport Layer**

Lapisan ini memegang peranan yang cukup penting pada komunikasi data. Pada lapisan ini dilakukan proses segmentasi paket. Segmentasi adalah proses pemecahan paket data sesuai ukuran *Maximum Transmission Unit (MTU)* yang

telah distandarkan. MTU adalah ukuran maksimal dari sebuah data yang dapat di transmisikan dalam 1 paket (Prakasa, 2018).

#### **2.1.4.5 Session Layer**

Lapisan ini berurusan dengan hubungan antara komputer pengirim dan penerima. Pada lapisan inilah dipastikan setiap pengguna akan mendapatkan informasi yang dimintanya meskipun banyak pengguna mengakses *server* secara bersamaan. Setiap pengguna akan mendapatkan identitas khusus sehingga tidak terjadi kekeliruan pengiriman data (Prakasa, 2018)

#### **2.1.4.6 Presentation Layer**

Lapisan ini menerima data dari lapisan *Application* untuk kemudian di proses terlebih dahulu sebelum diteruskan ke lapisan *session*. Salah satu proses yang cukup vital di lapisan ini adalah pemampatan / *compress* data. Tujuan dari pemampatan data adalah agar data yang dikirimkan dapat berukuran sekecil mungkin. Pada perangkat komputer penerima, data akan di *extract* terlebih dahulu sebelum di teruskan ke lapisan *Application* (Prakasa, 2018).

#### **2.1.4.7 Application Layer**

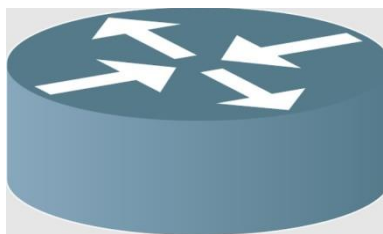
Pada lapisan *Application* memberikan landasan kepada *software* yang akan menggunakan jaringan komputer seperti *web browser*, *email client*, *ftp client* dan lain sebagainya (Prakasa, 2018).

## **2.2 Teori Khusus**

Teori khusus yang digunakan peneliti pada penelitian ini yaitu *Router Mikrotik*, *Virtual Private Network*, dan *Tunnel*.

### 2.2.1 Router Mikrotik

Router berfungsi untuk menghubungkan dari satu jaringan ke jaringan yang lain. Penerapan *Router* berada pada lapisan *Network* di model OSI. *Router* dianggap memiliki kemampuan *Routing*, dalam arti *router* dapat mengetahui kemana rute perjalanan (*Packet*) akan dilewatkan (Sofana Iwan, 2017). Simbol khusus untuk menandakan sebuah perangkat *Router* digambarkan seperti dibawah ini.



**Gambar 2. 17** Simbol Router

#### 2.2.1.1 Sejarah Mikrotik

Mikrotik dibangun pada tahun 1995 oleh Jhon Trully dan Arnis Riesktinis, sampai saat ini berbagai perangkat mikrotik telah tersebar penjualannya diseluruh dunia. Perusahaan mikrotik mengembangkan sebuah sistem operasi *Router* yang berfitur lengkap yang disebut *RouterOS*.

Tahap perkembangan mikrotik selanjutnya pada tahun 2002, yaitu perusahaan mikrotik memproduksi perangkat keras dengan merek *RouterBoard*. Dari berjalannya waktu, *RouterBOARD* mengembangkan desain dan fitur baru untuk membantu perusahaan kecil, penyedia jasa layanan internet, dan penyedia jasa layanan nirkabel untuk mengembangkan usahanya.

### 2.2.1.2 Mikrotik RouterOS

Mikrotik *RouterOS* merupakan suatu sistem operasi yang diperuntukkan sebagai *network router*. Mikrotik *RouterOS* sendiri adalah sistem operasi dan perangkat lunak yang dapat membuat komputer biasa menjadi sebuah *router network* yang andal dan memiliki banyak fitur menarik (Sofana Iwan, 2017).

### 2.2.1.3 Mikrotik License

Mikrotik *RouterOS* menerapkan sebuah sistem operasi berlisensi. Untuk dapat menggunakan seluruh fitur hebat secara penuh yang diuraikan dari fitur level 0 hingga level 6 sampai saat ini, harus membeli lisensi yang akan digunakan satu lisensi hanya *valid* untuk satu buah harddisk.

### 2.2.1.4 Mikrotik RouterBOARD

Sebagian besar orang menyebut Mikrotik *Router* sebagai *RouterBOARD*.

Mikrotik *Router* dibagi 2 kelompok, yaitu:

- A. Integrated yaitu sebuah perangkat *router* lengkap dengan *casing* dan *power supply*. Contoh nya *RB750*, *RB751U-2HnD*.



**Gambar 2. 18** Mikrotik RB750

B. *RouterBOARD* yaitu sebuah *motherboard* tidak memiliki *power supply*, *interface*, dan *casing*. Jenis *router* seperti ini dapat di kostum untuk disesuaikan dengan kebutuhan penggunaannya. Contohnya RB411 dan RB800.



**Gambar 2. 19** Mikrotik RB800

### **2.2.2 Virtual Private Network**

*Virtual Private Network* adalah sebuah metode dalam membangun jaringan untuk menghubungkan antara node jaringan secara aman dan terenkripsi dengan memanfaatkan jaringan publik (Sofana Iwan, 2017). Secara garis besar VPN ini bertujuan untuk menghubungkan suatu jaringan lokal yang lokasinya berjauhan tanpa harus menanam kabel yang sangat panjang untuk bisa saling terkoneksi.

### **2.2.3 Tunnel**

*Tunnel* merupakan sebuah teknik yang digunakan untuk memungkinkan aliran data dapat diolah melalui *network* yang berbeda jenis (Sofana Iwan, 2017). Kegunaan *tunnel* dianggap perlu dalam mengamankan aliran data yang saling

terhubung melalui *network* sehingga dalam pengaksesan data hanya dapat diakses oleh pengguna yang memiliki hak dalam pengaksesan data.

Terdapat kurang lebih ada 5 buah *tunneling protocol* yang cukup populer (Sofana Iwan, 2017) diantaranya.

1) Point to Point Tunneling Protocol (PPTP)

Protocol ini merupakan salah satu protokol *tunnel* Layer 3 OSI yang paling umum. Sistem dan perangkat seperti *windows*, *Mac OSX*, Mikrotik *router*, dan perangkat PPTP *Client* yang lain nya telah mendukung PPTP ini.

2) Layer 2 Tunneling Protocol (L2TP)

Protokol ini merupakan pengembangan dari PPTP dan hanya bekerja di Layer 2 OSI. Ketika melakukan komunikasi, L2TP menggunakan UDP *port* 1701

3) Ethernet over Internet Protocol (EoIP)

Protokol ini bekerja pada protokol *tunnel* Layer 2 milik mikrotik dan dapat melakukan bridge 2 buat jaringan melalui *internet*. Protokol ini tidak dienkripsi dan dapat bekerja sangat cepat namun kekurangannya tidak aman.

4) Multiprotocol Label Switching and Virtual Private LAN Service (MPLS/VPLS)

Protokol *Tunnel* yang kinerjanya cukup ampuh. Protokol ini banyak diimplementasikan oleh ISP yang jaringannya cukup kompleks.

5) Point to Point Tunneling Protocol over Ethernet

Protokol ini terdapat di Layer 2 OSI. Kinerjanya dapat membatasi akses jaringan, melalui otentikasi sentral, dan *automatic provisioning* serta mendukung *ip adress* khusus yang disebut dengan *point to point addressing*.



## 2.3 Tools

Peneliti menggunakan beberapa *tools*, komponen perangkat jaringan, atau *software* tambahan yang akan digunakan pada perancangan *Virtual Private Network*.

### 2.3.1 Mikrotik RouterBoard RB750

Perangkat tambahan yang diperlukan peneliti dalam perancangan virtual private network salah satunya perangkat mikrotik routerboard750. Ukuran perangkat ini agak kecil. Perangkat ini memiliki 5 buah port ethernet 10/100 yang memiliki prosesor atheros 400MHz, lisensi level 4 dan ukuran adaptor 12 volt. Berikut ini tampilan spesifikasi mikrotik yang akan digunakan.

**Tabel 2. 1** Spesifikasi MikroTik Yang Digunakan

Spesifikasi Routerboard 750	
CPU	AR7161 680/800MHz CPU
Memory	32MB DDR SDRAM onboard memory
Boot Loader	RouterBOOT
Data Storage	64MB onboard NAND memory chip
Ethernet	Five 10/100/1000 gigabit ethernet ports (with switch chip)
Mini PCI	None
Extras	Reset switch, Beeper
Serial Port	No Serial Port
LEDs	Power, NAND activity, 5 Ethernet LEDs
Power Option	Power over Ethernet: 9-28V DC (except power over datalines), Power jack: 9.28V DC
Dimensions	133x89x28mm, Weight without packaging and cables: 130g
Power Consumption	Up to 3W
Operating System	MikroTik RouterOS v3, Level 4 License

**Sumber:** (www.citraweb.com)

Dari Spesifikasi yang tertera di tabel 2.1, dapat diketahui bahwa mikrotik Rb750 tidak memiliki fitur pemancar Wi-Fi. Tampilan gambar dibawah ini menunjukkan mikrotik yang digunakan peneliti untuk merancang jaringan komputer yang berada dikantor Cv. Celcomindo.



**Gambar 2. 20** Perangkat MikroTik RB750

**Sumber:** (Peneliti, 2021)

### **2.3.2 Tp Link Wi-Fi Router Archer C24**

Tp-link ini digunakan sebagai akses poin untuk perangkat-perangkat yang berada pada jaringan lokal kantor agar saling terhubung melalui wireless di jaringan lokal tersebut. Perangkat-perangkat yang terdapat pada kantor, diharuskan terhubung melalui Wi-Fi, tidak menggunakan kabel. Hal ini merupakan keinginan dari direktur Cv. Celcomindo. Mikrotik Rb750 tidak memiliki fasilitas Wi-Fi, oleh karena itu penambahan perangkat Tp link Wifi-Rotuter Archer C24 sangat dibutuhkan. Tp link ini memiliki 1 buah ethernet port Wan, 4 buah ethernet port lan dan 4 antena Wi-Fi. Perangkat ini dapat dijadikan sebagai Router, Akses Poin, dan Extender Multiple Modes. Dibawah ini tampilan spesifikasi Tp link Wi-Fi Router yang digunakan.

**Tabel 2. 2** Spesifikasi Tp Link Wi-Fi Router Yang Digunakan

Spesifikasi Tp Link Wi-Fi Router Archer C24	
<i>Wireless</i>	433 Mbps (5 GHz) + 300 Mbps (2.4 GHz)
Antennas	4x Fixed Omni-Directional Antennas
Ports	1x 10/100 Mbps WAN Port + 4x 10/100 Mbps LAN Ports
Dimensions	4.5 x 4.2 x 1.0 in (115 x 106.7 x 24.3mm)

**Sumber:** (Peneliti, 2021)

Tabel 2.2 menunjukkan spesifikasi yang dimiliki perangkat Tp link Wi-Fi Router yang digunakan, dibawah ini tampilan gambar perangkat Tp link Wi-Fi Router yang akan dijadikan sebagai Access Point untuk perangkat yang berada di jaringan lokal kantor tersebut.

**Gambar 2. 21** Perangkat Tp Link Wi-Fi Router

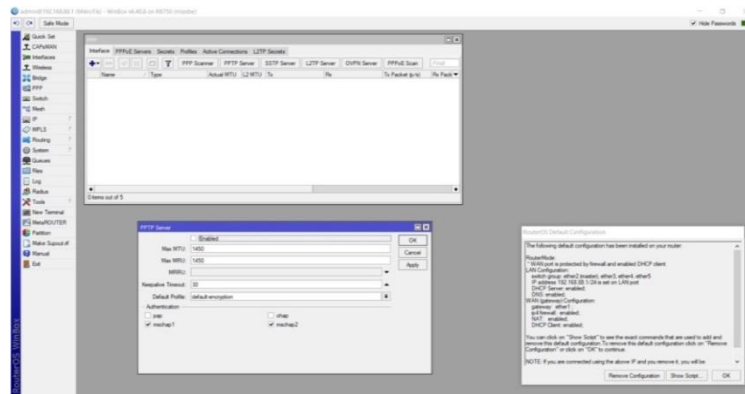
**Sumber:** (Peneliti, 2021)

### 2.3.3 WinBox

*WinBox* ini aplikasi desktop pada OS yang digunakan untuk akses perangkat keras mikrotik. Aplikasi ini mempermudah pengguna dalam

mengkonfigurasi mikrotik sehingga pengguna tidak terlalu sulit dalam menjalankan perintah atau fitur yang ada di mikrotik.

*Winbox* diartikan sebuah perangkat lunak yang digunakan dalam melakukan *remote* ke *server* mikrotik yang dimiliki dengan tampilan mode GUI (Didi Susianto, 2016).



**Gambar 2. 22** Tampilan WinBox Ketika Login Ke Mikrotik

**Sumber:** (Peneliti, 2021)

### 2.3.4 Kabel UTP dan RJ45

Komponen ini sudah digabungkan diantaranya menggunakan kabel UTP CAT 5e dan RJ45. Komponen ini digunakan untuk menghubungkan mikrotik dengan laptop dalam tujuan mengkonfigurasi mikrotiknya dengan bantuan WinBox.



**Gambar 2. 23** Kabel UTP Cat 5e dan Rj45

**Sumber:** (Peneliti, 2021)

#### **2.4 Penelitian Terdahulu**

Penelitian terdahulu merupakan sebagai acuan peneliti dalam melakukan penelitian ini. Keterkaitan dengan judul, metode, dan masalah penelitian yang berhubungan oleh penelian ini dengan topik Perancangan dan Implementasi *Virtual Private Network* Dengan Mikrotik.

Penelitian (Elezi & Raufi, 2015) ISSN: 1938-1948 dengan judul *Conception of Virtual Private Network using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption*. Kesimpulan dari hasil yang didapat pada penelitian tersebut bahwa peningkatan enkripsi atau kemandan data menyebabkan penurunan kecepatan eksekusi yang signifikan. Contohnya dalam hal peningkatan keamanan atau pemilihan tunnel yang lebih bagus, semakin tinggi tingkat keamanan nya semakin tinggi spesifikasi komponen router yang dibutuhkan.

Penelitian (Supendar, 2016) Vol. 3 ISSN: 2527-8777 dengan judul *Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik*. Hasil

kesimpulan yang didapat atas penelitian tersebut bahwa VPN rentan terhadap serangan seperti DoS atau *Denial of Service* dan cara mengatasinya dengan memblokir protokol ICMP sehingga *IP Public* tidak dapat di *ping*. Pada evaluasi keamanan dibuktikan bahwa penggunaan VPN dengan protokol PPTP terdapat proses kompres data, enkapsulasi dan enkripsi.

Pada penelitian (Mufida, Irawan, & Chrisnawati, 2017) Vol. 16 ISSN: 1858-4144 yang berjudul *Remote Site Mikrotik VPN Dengan Point to Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta*. Kesimpulan dari hasil penelitian tersebut bahwa jaringan kantor yayasan dengan jaringan sekolah dapat terhubung dengan VPN yang memanfaatkan internet dan pengambilan maupun pengiriman data tidak lagi dilakukan secara manual seperti melakukan email melainkan menggunakan jaringan VPN yang langsung terhubung ke jaringan lokal antara kantor yayasan dengan sekolah.

Penulis (Surantha & Rino, 2018) melaksanakan penelitian dengan judul *Secure Portable Virtual Private Network with Rabbit Stream Cipher Algorithm*. Kesimpulan dari penelitian yang dilakukan dengan simulasi bahwa algoritma *Rabbit* mencapai kecepatan data tertinggi, konsumsi memori terendah, dan pemanfaatan CPU terendah diantara semua algoritme yang dievaluasi yaitu *AE-256*, *Triple DES (3DES)*, *Camelia 256*, dan *SEED*. Algoritma *Rabbit* sesuai untuk diterapkan karena memiliki kebutuhan daya rendah dan unggul dari perbandingan algoritme lain yang telah dibandingkan dengan algoritma *Rabbit*.

(Maryanto, Maisyaroh, & Santoso, 2018) melakukan penelitian yang berjudul *Metode Internet Protocol Security (IPSec) Dengan Virtual Private*

*Network* (VPN) Untuk Komunikasi Data. Kesimpulan dari hasil penelitian dapat dianalisa bahwa penggunaan VPN dengan protokol IPSec menjadi solusi jaringan yang aman karna data berjalan pada jaringan publik. Selain itu pemanfaatan keamanan jaringan *firewall*, *Intrusion Prevention System (IPS)*, *McAfee Mail gateway* beserta antivirus *McAfee Complete EndPoint Protection* sangat membantu dalam menangani gangguan keamanan jaringan pada jaringan VPN.

Penelitian yang berjudul Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna yang diteliti (Putra, Jordy Lesmana, Indriyani, Luthfi, Angraini, 2018) Vol. 2 ISSN: 2549-7421, mendapat kesimpulan bahwa keamanan jaringan komputer menggunakan VPN dengan metode PPTP akan mempermudah pekerjaan bagian IT untuk dapat mengontrol dan mengatasi permasalahan jaringan yang ada di perusahaan dan mengontrol nya dari jarak jauh tanpa harus datang ke perusahaan.

Penelitian (Hidayatulloh & Wahyudin, 2019) Vol. 5 ISSN: 2550-0120 dengan judul Perancangan *Wide Area Network* (WAN) Dengan Teknologi *Virtual Private Network* (VPN). Kesimpulan hasil dari penelitian mereka bahwa user yang menggunakan hak akses VPN dapat melakukan pengiriman data dan *Share Folder* dan untuk user yang tidak memiliki hak akses VPN hanya mampu melakukan koneksi sampai *router* saja dan pengiriman data hanya user yang memiliki hak akses data saja yang dapat melakukan nya.

(Zarkasyi, Agus, Permana, Dillak, & Kom, 2018) Vol 4 ISSN: 2442-5826 dengan judul Implementasi *Virtual Private Network* (VPN) Server Dengan Menggunakan Mikrotik OS Di PT. Charisma Persada Nusantara. Kesimpulan dari

penelitian yang dilakukan bahwa semakin banyak user yang menggunakan VPN akan semakin meningkat kinerja VPN Server.

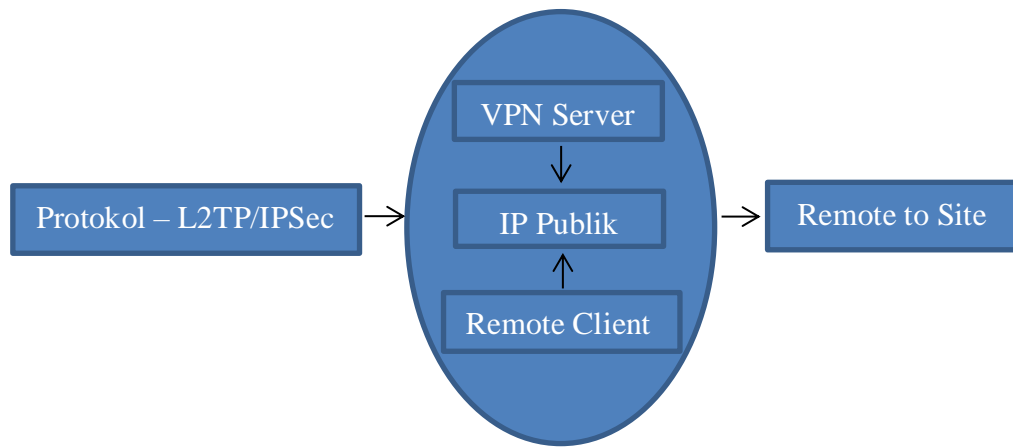
Penelitian (Dewi, 2020) Vol 8 ISSN:2657-0793 yang berjudul Keamanan Jaringan Menggunakan VPN (*Virtual Private Network*) Dengan Metode PPTP (*Point To Point Tunneling Protocol*) Pada Kantor Desa Kertaraharja Ciamis. Kesimpulan dari penelitian yang dilakukan bahwa penerapan vpn yang dilakukan memiliki dampak positif karena pertukaran informasi atau pengolahan data yang berada dikantor desa kertaraharja menjadi lebih fleksibel dan memudahkan teknisi jaringan dikantor tersebut untuk memonitoring jaringan yang berjalan pada masing-masing kantor.

(Sari, Sulistiyono, & Kemala, 2020) melakukan penelitian yang berjudul Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik. Vol 7 ISSN: 2597-9922. Kesimpulan dari pelaksanaan penelitian yang dilakukan bahwa VPN yang dirancang sesuai dengan yang diharapkan ditambah keamanan data pada protokol yang digunakan yaitu IPSec yang dapat mengenkripsi data yang keluar masuk sehingga keamanan data dapat terjamin.

## **2.5 Kerangka Pemikiran**

Kerangka pemikiran pada penelitian ini bahwa perancangan virtual private network menggunakan protokol L2tp/IPSec melalui proses koneksi dari remote client ke VPN Server terhadap ip publik yang berada dimikrotik yang akan digunakan untuk remote to site ke perangkat yang berada dijaringan lokal kantor Cv. Celcomindo tersebut.





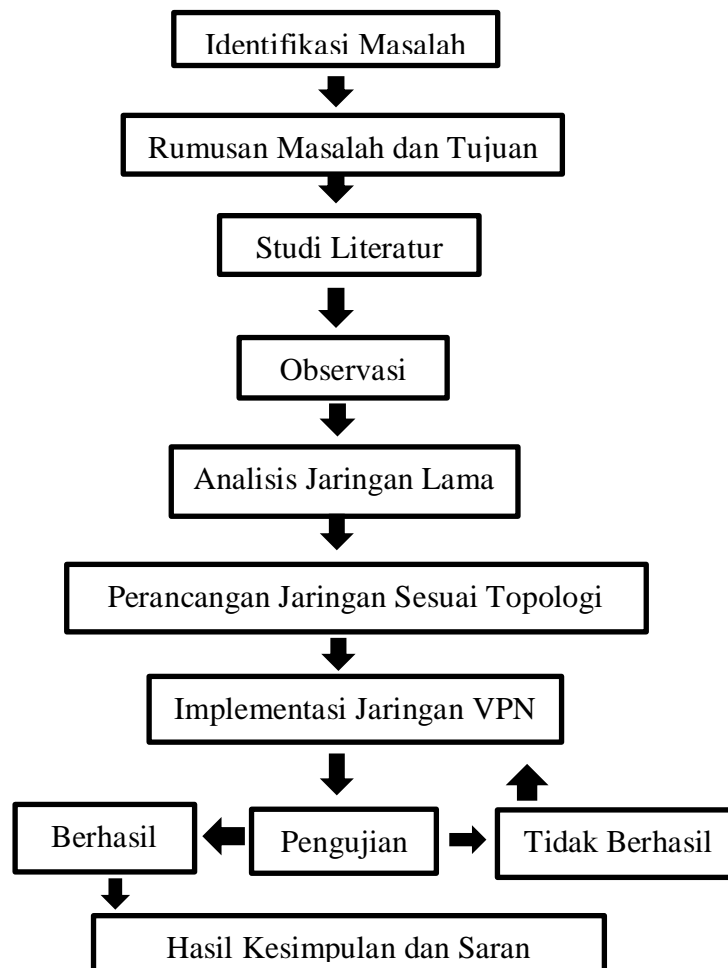
**Gambar 2. 24** Kerangka Pemikiran

**Sumber:** (Peneliti, 2021)

**BAB III**  
**METODE PENELITIAN**

**3.1 Desain Penelitian**

Pada penelitian ini, desain penelitian dibuat untuk menjelaskan gambaran dari proses awal pembuatan penelitian hingga menuju ke hasil penelitian oleh suatu proses penelitian yang dilakukan.



**Gambar 3. 1** Desain Penelitian

**Sumber:** (Peneliti, 2021)

Dari urutan gambar desain penelitian diatas pembahasannya sebagai berikut.

### **3.1.1 Identifikasi Masalah**

Tahap identifikasi Masalah, peneliti mengidentifikasi suatu permasalahan yang sedang terjadi di kantor CV. Celcomindo dan berharap dapat menyelesaikan apa yang menjadi hambatan atau permasalahan yang ada dikantor tersebut.

### **3.1.2 Rumusan Masalah dan Tujuan**

Pada tahap Rumusan Masalah, peneliti menyusun perumusan masalah yang di dapat dari keterangan pihak kantor CV. Celcomindo dan merincikan permasalahan permasalahan apa yang terjadi guna mencari solusi atau tujuan untuk menyelesaikan permasalahan tersebut.

### **3.1.3 Studi Literatur**

Setelah mengetahui permasalahan yang terjadi di lokasi penelitian, peneliti melakukan Studi Literatur yang berkaitan dengan permasalahan yang ada. Didalam suatu penelitian atau penyusunan karya ilmiah, peneliti wajib mengetahui teori-teori terkemuka yang berkaitan dengan permasalahan yang akan ditangani.

### **3.1.4 Observasi**

Pengumpulan data pada penelitian ini dilakukan dengan cara observasi, yaitu peneliti langsung menuju kelokasi penelitian untuk menganalisa permasalahan yang ada. Menganalisa jaringan lama yang sudah dibangun, merancang skema jaringan yang akan dibangun untuk perancangan VPN,

menganalisa kendala-kendala yang akan terjadi pada proses penelitian dan sebagainya.

### **3.1.5 Analisis Jaringan Lama**

Mengenai permasalahan yang ada di CV. Celcomindo, peneliti menganalisa jaringan lama atau yang sudah dirancang di kantor tersebut. Tujuannya untuk mengetahui apa saja yang diperlukan untuk perancangan jaringan selanjutnya yang akan dibangun. Adapun analisa jaringan komputer yang sudah ada di kantor tersebut, analisa yang dilakukan berupa bentuk topologi jaringan apa yang digunakan di kantor tersebut, apa saja perangkat yang digunakan, bagaimana spesifikasi perangkat-perangkat yang ada di kantor tersebut dan sebagainya.

### **3.1.6 Perancangan Jaringan Sesuai Topologi**

Ditahap ini setelah peneliti menganalisa jaringan yang sudah dibangun sebelumnya di kantor tersebut, peneliti lanjut ke tahap rancangan jaringan yang akan dibangun atau diusulkan. Sebelum menentukan rancangan jaringan VPN yang akan dibangun, peneliti membuat topologi jaringan yang diusulkan untuk dibangun. Ditahap ini, peneliti menentukan posisi-posisi perangkat sesuai dengan topologi untuk akses jaringan internet menggunakan ip publik serta posisi perangkat-perangkat yang berada di jaringan lokal melalui topologi jaringan yang dibuat.

### **3.1.7 Implementasi Jaringan VPN**

Setelah membuat topologi jaringan yang diusulkan dan menyusun perangkat-perangkat yang dibutuhkan, kemudian peneliti mengimplementasikan

tahapan-tahapan jaringan VPN yang akan dirancang dikantor tersebut dengan mengkonfigurasi hal-hal yang berkaitan dengan perancangan jaringan diantaranya mengonfigurasi mikrotik untuk jaringan internet dengan ip publik, menyetting alamat ip untuk jaringan lokal serta mengonfigurasi tp link sebagai akses poin. Kemudian peneliti memastikan apakah perancangan sudah dilakukan dengan baik dan benar atau belum. Lalu peneliti memastikan bahwa jaringan komputer lokal sudah sesuai dengan yang diharapkan dan sudah dikonfigurasi semestinya dimana jaringan komputer lokal dikantor tersebut juga sudah memiliki akses untuk ke jalur jaringan internet dengan konfigurasi yang dilakukan di mikrotik dan VPN server nya telah dirancang.

### **3.1.8 Pengujian**

Ditahap ini, penelitian melakukan pengujian koneksi virtual private server yang dirancang apakah sudah berjalan dengan baik atau belum, pengujian mengakses mikrotik melalui jaringan virtual private server dengan menggunakan ip vpn dan ip lokal pada jaringan tersebut, pengujian ping kebeberapa perangkat yang terhubung ke jaringan lokal, pengujian mengakses port 80 pada http tp link dan pengujian remote desktop serta melakukan pertukaran file pada remote desktop. Fokus penelitian ini adalah bagaimana mengatasi permasalahan dikantor, dimana data atau resource yang ada di jaringan lokal kantor tersebut dapat diakses dari jarak jauh atau dari luar kantor yang posisi lokasi nya berjauhan dengan cara remote akses serta bagaimana cara mengonfigurasi jaringan yang dirancang. Jika pengujian belum berhasil atau belum sesuai dengan harapan yang di inginkan, peneliti akan kembali ke langkah implementasi jaringan jika pada saat pengujian

belum berhasil dan mengkonfigurasi ulang perangkat yang digunakan sampai pada tahapan pengujian ini berhasil dilakukan.

### **3.1.9 Hasil Kesimpulan dan Saran**

Pada tahapan ini, setelah tahap pengujian berhasil dilakukan dan sesuai dengan harapan maka peneliti akan menyusun kesimpulan dari hasil penelitian dan saran yang didapat dari perancangan jaringan yang dilakukan. Kesimpulan yang diuraikan berupa hasil yang didapatkan dari proses perancangan jaringan tersebut yang dilakukan peneliti dalam menyelesaikan permasalahan terhadap penelitian yang dilakukan. Menguraikan saran-saran yang perlu diperhatikan mengenai penelitian ini agar kedepannya rancangan jaringan VPN ini bisa dikembangkan dari apa kekurangan yang diperlukan untuk mengembangkan perancangan jaringan VPN ini dilokasi penelitian tersebut.

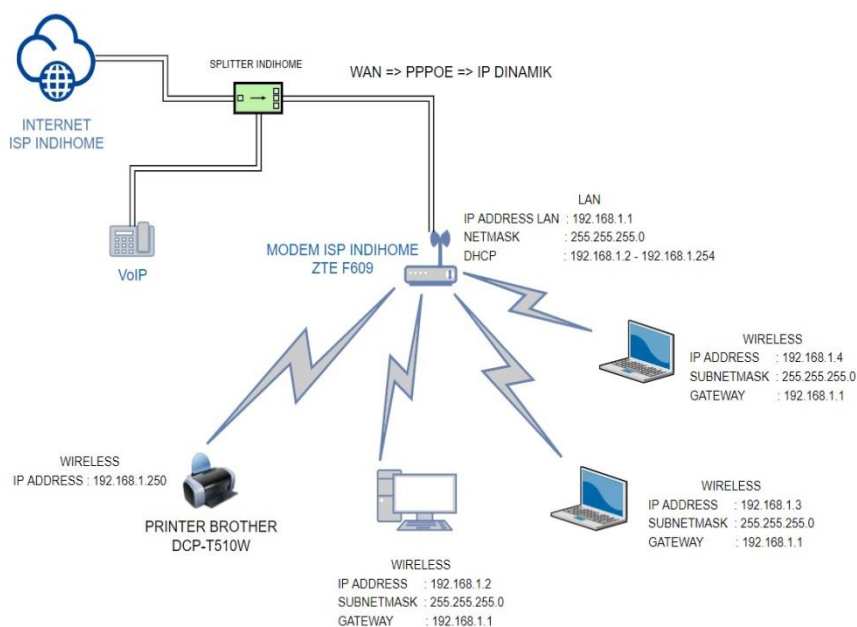
### **3.2 Analisis Jaringan Lama atau Yang Sedang Berjalan**

Pada sub bab sebelumnya yang telah disampaikan oleh peneliti mengenai desain penelitian, kemudian disub bab ini peneliti akan menjelaskan rincian mengenai analisis jaringan lama atau jaringan yang sudah berjalan dikantor tersebut sebelum dirancangnya perancangan jaringan VPN. Dalam proses analisis ini, peneliti langsung meneliti kelengkapan ditempat lokasi penelitian yang akan dilakukan. Analisis yang dilakukan diantaranya bagaimana bentuk topologi yang sudah ada dikantor tersebut, kantor tersebut menggunakan jasa layanan *Internet Service Provider* apa, bagaimana spesifikasi detail hardware jaringan yang ada dikantor tersebut, software seperti apa yang digunakan seperti Operating

System ataupun aplikasi yang digunakan yang perlu diuraikan secara rinci mengenai jaringan komputer yang ada dikantor tersebut.

### 3.2.1 Topologi Jaringan Yang Sedang Berjalan

Peneliti mengamati letak perangkat jaringan yang ada dikantor tersebut beserta komputer dan perangkat lain nya yang saling terhubung. Gambaran topologi jaringan yang sedang berjalan dikantor celcomindo seperti gambar dibawah ini.



**Gambar 3. 2** Topologi Jaringan Yang Sedang Digunakan

**Sumber:** (Peneliti, 2021)

Aplikasi yang digunakan peneliti untuk menggambar topologi jaringan diatas menggunakan software Draw.Io. Dari bentuk topologi jaringan diatas, penjelasannya bahwa CV. Celcomindo menggunakan jasa layanan Internet Service Provider milik Indihome. Perangkat Splitter digunakan untuk

memisahkan jalur kabel internet yang akan dihubungkan ke perangkat ZTE f609 dan jalur kabel telephone yang akan dihubungkan ke perangkat telepon. Pada modem ZTE f609, terdapat konfigurasi yang akan menghubungkan jaringan lokal ke wan dengan pppoe yang otomatis didapat dari ISP indihome dengan ip dinamik. Modem ZTE f609 akan mengonfigurasi settingan untuk ip lokal yang berada dikantor dengan *network* ip address 192.168.1.1 dan dhcp client berada pada rentang ip 192.168.1.2 – 192.168.1.254 dengan gateway 192.168.1.1. Dapat dilihat pada gambar topologi diatas terdapat perangkat-perangkat yang saling terhubung ke ZTE f609 diantaranya 1 unit komputer, 2 unit laptop, dan printert. Perangkat-perangkat tersebut mendapatkan alamat ip sesuai ip dhcp yang diberi zte f609 dan perangkat tersebut terhubung dengan media penghantar wireless. Peneliti mendapat alasan mengapa perangkat-perangkat tersebut terhubung melalui wireless dan tidak menggunakan kabel, karena untuk memudahkan proses pemindahan posisi perangkat jika ingin dilakukan oleh direktur CV. Celcomindo






### **3.2.2 Spesifikasi Hardware dan Software Yang Sedang Dipakai**

Spesifikasi hardware yang digunakan dilokasi penelitian diantaranya terdapat Modem ZTE F609 yang digunakan untuk mengonfigurasi jaringan WAN dan LAN. Terdapat 1 unit komputer dan 2 unit laptop dengan menggunakan OS windows 10 pro yang digunakan untuk melakukan suatu pekerjaan dikantor tersebut. Lalu terdapat 1 buah printer yang digunakan untuk mencetak atau scan suatu file dalam kegiatan pekerjaan dikantor tersebut. 1 unit komputer, 2 unit laptop dan 1 buah printer tersebut terhubung ke modem ZTE F609 melalui media penghantar wireless dan masing-masing mendapatkan alamat ip local dari modem



ZTE F609 untuk saling terhubung sebagai jaringan lokal. Dibawah ini akan diuraikan dalam bentuk tabel.

**Tabel 3. 1** Spesifikasi Hardware dan Software Yang Digunakan

No	Hardware	Software	Gambar	Keterangan
1	ZTE F609	Software Version V7.0.1		Konfigurasi jaringan lokal dan jaringan wan
2	Komputer Lenovo Intel(R) Core(TM) i3- 2120	Windows 10 Pro 64 bit.		Komputer untuk pekerjaan kantor
3	1 Unit Laptop Hp Envy DV6 Core i7-3630qm	Windows 10 Pro 64 bit		Laptop untuk pekerjaan kantor
4	1 Unit Laptop Lenovo x240 Core i5	Windows 10 Pro 64 bit		Laptop yang digunakan untuk pekerjaan kantor
5	1 Unit Printer Brother DCP- T510W	Driver & Software Packet Version B2		Printer yang digunakan untuk keperluan kantor

**Sumber:** (Peneliti, 2021)

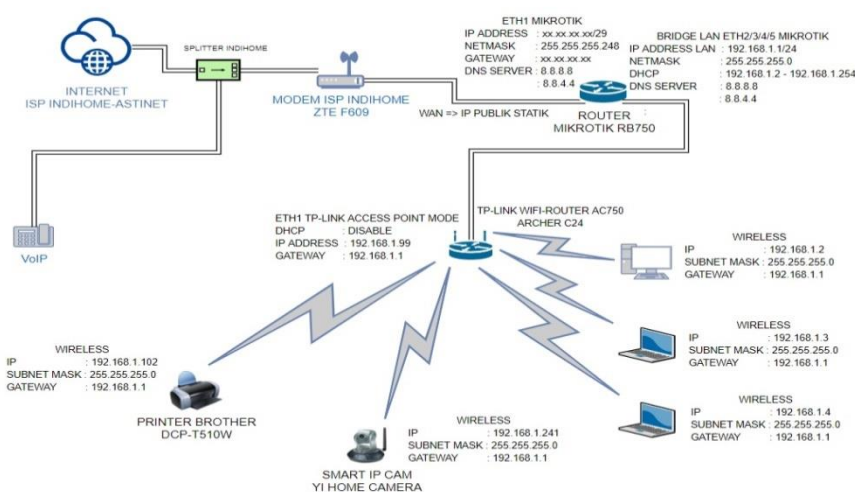
### 3.3 Rancangan Jaringan Yang Dibangun atau Diusulkan

Pada tahap ini, peneliti menguraikan secara rinci mengenai rancangan jaringan yang akan dibangun atau diusulkan dikantor tersebut yang sebelum nya sudah melakukan simulasi pada software *Cisco Packet Tracer*. Rincian nya pada sub bab ini, bentuk topologi seperti apa yang akan digunakan dalam perancangan

yang akan dibangun, apa saja perangkat tambahan yang digunakan dalam perancangan jaringan yang dibangun, menjelaskan rincian spesifikasi perangkat-perangkat yang digunakan apakah ada tambahan perangkat baru atau tetap memakai perangkat lama dan sebagainya.

### 3.3.1 Topologi Jaringan Yang Baru

Setelah menganalisis jaringan yang sedang berjalan dikantor tersebut dan menyimpulkan maksud dan tujuan dari permasalahan yang disampaikan pada penelitian yang dilakukan bahwa akan dirancangnya perancangan jaringan virtual private network dengan mikrotik. Topologi yang digunakan dalam perancangan jaringan tersebut seperti gambar dibawah ini.



**Gambar 3.3** Topologi Jaringan Yang Akan Dirancang

**Sumber:** (Peneliti, 2021)

Gambar topologi jaringan diatas peneliti menggunakan aplikasi Draw.Io untuk menggambar topologi tersebut. Topologi diatas dapat diperhatikan bahwa CV. Celcomindo akan menggunakan ISP Astinet untuk terhubung ke internet



karena untuk merancang virtual private network dibutuhkannya IP Publik dengan berlangganan di ISP Astinet. Kita perhatikan bahwa perangkat-perangkat yang terhubung di jaringan lokal kantor tersebut tidak jauh berbeda dengan topologi jaringan yang sebelumnya digunakan. Pada topologi diatas, untuk modem ZTE f609 tidak dilakukan konfigurasi karena hanya digunakan sebagai penghubung ke mikrotik. Untuk konfigurasi jaringan WAN dan Jaringan LAN dilakukan di perangkat mikrotik beserta perancangan jaringan VPN nya.

Perangkat tambahan antara lain router mikrotik rb750, perangkat tp-link wireless-router yang akan digunakan sebagai bridge access point agar perangkat-perangkat lokal dapat terhubung ke mikrotik, dan penambahan perangkat cctv camera. Kita perhatikan bahwa perangkat router mikrotik rb750 tidak ada fitur wireless nya dan hanya menggunakan perantara kabel, karena itu alasan mengapa ditambahkan perangkat tp-link wireless router.

### **3.3.2 Spesifikasi Hardware Dan Software**

Spesifikasi hardware dan software pada perangkat tambahan diantaranya terdapat MikroTik, Tp Link Wi-Fi Router, dan 1 perangkat Camera YI Home. Perangkat tambahan ini diletakkan sesuai dengan topologi jaringan yang diusulkan. Mikrotik digunakan untuk manajemen jaringan yang berada di kantor Cv. Celcomindo. Untuk Perangkat Tp Link Wi-Fi Router digunakan sebagai Access Point agar perangkat-perangkat yang terhubung ke jaringan lokal akan melalui Wi-Fi yang di setting di perangkat Tp Link Wi-Fi Router. Perangkat tambahannya seperti tabel dibawah ini.

**Tabel 3. 2** Spesifikasi Hardware dan Software Yang Digunakan

No.	Hardware	Software	Gambar	Keterangan
1.	Mikrotik rb750	RouterOS V3, Level 4 License		Konfigurasi jaringan wan, lan, dan virtual private network
2.	Tp-Link Wireless Router Archer C24	Firmware Version 1.0		Menghubungkan perangkat lokal melalui wireless
3	YI Home Camera	Firmware Version 2.1		Perangkat ini permintaan dari direktur kantor, sebagai cctv ruang kantor

**Sumber:** (Peneliti, 2021)

Untuk mengakses mikrotik, peneliti menggunakan aplikasi WinBox versi 3.27 yang akan digunakan dalam mengonfigurasi settingan mikrotik rb750.

### 3.3.3 Tahapan Rencana Implementasi Jaringan

Pada tahap ini setelah peneliti menggambarkan topologi jaringan yang akan dibangun, tahapan selanjutnya akan diuraikan dibawah ini.

1. Menyesuaikan dan menghubungkan letak posisi perangkat sesuai dengan topologi yang dibuat sebelum nya. Penambahan mikrotik rb750 yang

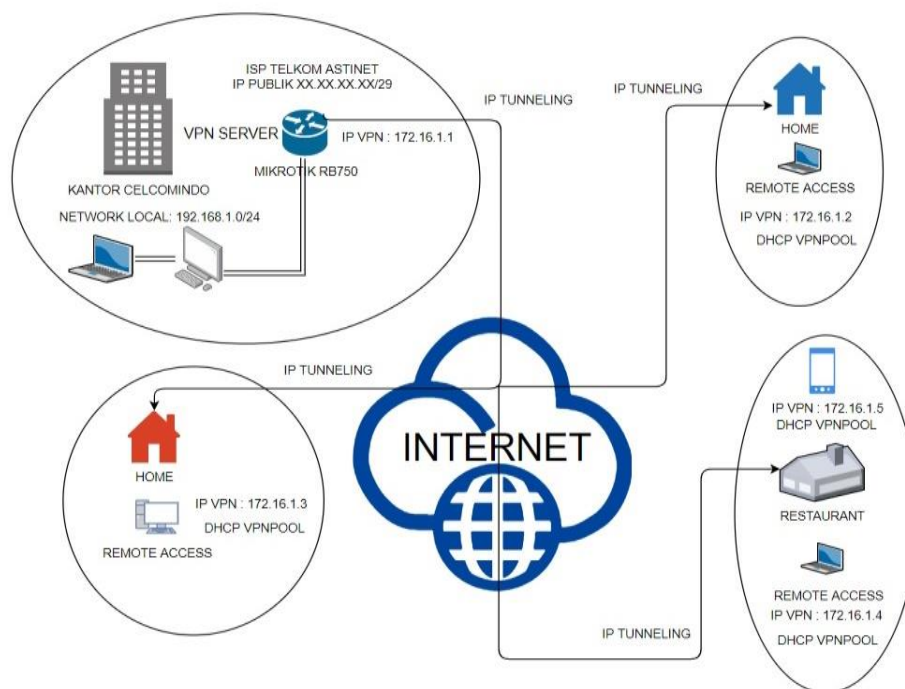
terhubung menggunakan kabel utp cat5e. Di ethernet 1 modem ZTE F609 akan dihubungkan kabel utp ke ethernet 1 yang terdapat di router mikrotik rb750. Kemudian, di ethernet 2 mikrotik akan dihubungkan kabel utp ke ethernet laptop untuk sementara karena mikrotik akan dikonfigurasi oleh peneliti. Lalu di ethernet 3 mikrotik akan dihubungkan kabel utp ke ethernet 1 tp-link wireless router dengan tujuan tp-link wireless router sebagai access point pemancar wifi untuk perangkat-perangkat yang berada dikantor.

2. Peneliti akan mengonfigurasi mikrotik diantaranya setting user login mikrotik agar mikrotik nya aman dari pihak luar yang ingin melakukan login pada mikrotik, setting IP Publik pada mikrotik yang didapat dari ISP Astinet, setting pembagian alamat ip address pada jaringan lokal sesuai dengan topologi yang sudah dibuat peneliti.
3. Setelah konfigurasi jaringan wan dan lan pada mikrotik selesai, tahap selanjutnya peneliti akan mensetting konfigurasi jaringan vpn yang akan dibangun pada mikrotik beserta jenis tunnel vpn yang digunakan.
4. Tahapan selanjutnya ketika konfigurasi sudah semestinya dilakukan, peneliti akan melakukan uji coba menggunakan fitur vpn tersebut dari luar area kantor dengan remote to site ke mikrotik dan remote desktop ke komputer lokal yang berada dikantor.

#### **3.3.4 Perbedaan Jaringan Yang Lama Dengan Yang Baru**

Perbedaan jaringan yang lama dengan yang baru dari segi ruangan hanya menambah beberapa perangkat seperti mikrotik rb750 dan perangkat tp-link

wireless-router untuk dijadikan sebagai wireless access point. Dari segi topologi bisa dilihat di topologi jaringan yang sedang berjalan, topologi jaringan yang baru, dan topologi jaringan VPN yang akan ditampilkan pada gambar dibawah ini.



**Gambar 3.4** Topologi Jaringan Virtual Private Network

**Sumber:** (Peneliti, 2021)

### 3.4 Lokasi dan Jadwal Penelitian

Disini Peneliti akan menjelaskan rincian Lokasi dan Jadwal Penelitian yang dilakukan dengan menyertakan foto kantor celcomindo dari depan dan map tempat dimana lokasi penelitian kantor tersebut berada serta menyertakan jadwal penelitian yang dilakukan dengan menggunakan tabel.

### 3.4.1 Lokasi

Lokasi tempat penelitian untuk perancangan *virtual private network* dilakukan di CV. Celcomindo yang beralamat di Ruko Omasen AA2 No.5, Batam Center.



**Gambar 3. 5** Kantor CV. Celcomindo

**Sumber:** (Peneliti, 2021)

Lokasi kantor CV. Celcomindo jika ditelusuri dari google map akan tampil seperti gambar dibawah ini.



**Gambar 3. 6** Lokasi Penelitian Melalui Google Map

**Sumber:** (Peneliti, 2021)

### 3.4.2 Jadwal Penelitian

Dalam penyusunan penelitian ini, peneliti menyertakan jadwal penelitian yang dilakukan dari awal hingga akhir. Dengan adanya jadwal penelitian ini, peneliti dapat menargetkan waktu untuk fokus terhadap penelitian yang dilakukan agar selesai tepat sesuai waktu yang dijadwalkan.

**Tabel 3. 3** Jadwal Penelitian

Kegiatan Penelitian	Maret				April				Mei				Juni				Juli				Agustus			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Menemukan Permasalahan dan Pemilihan Judul	■																							
Pengajuan Judul Penelitian	■	■	■																					
Penyusunan BAB I	■	■	■	■	■	■	■																	
Pengajuan Surat Penelitian dan Penyusunan BAB II				■	■	■	■	■	■	■	■													
Penelitian Dilapangan dan Penyusunan BAB III				■	■	■	■	■	■	■	■													
Penelitian Dilapangan dan Penyusunan BAB IV									■	■	■	■	■	■	■	■								
Penyusunan BAB V									■	■	■	■	■	■	■	■								

**Sumber:** (Peneliti, 2021)